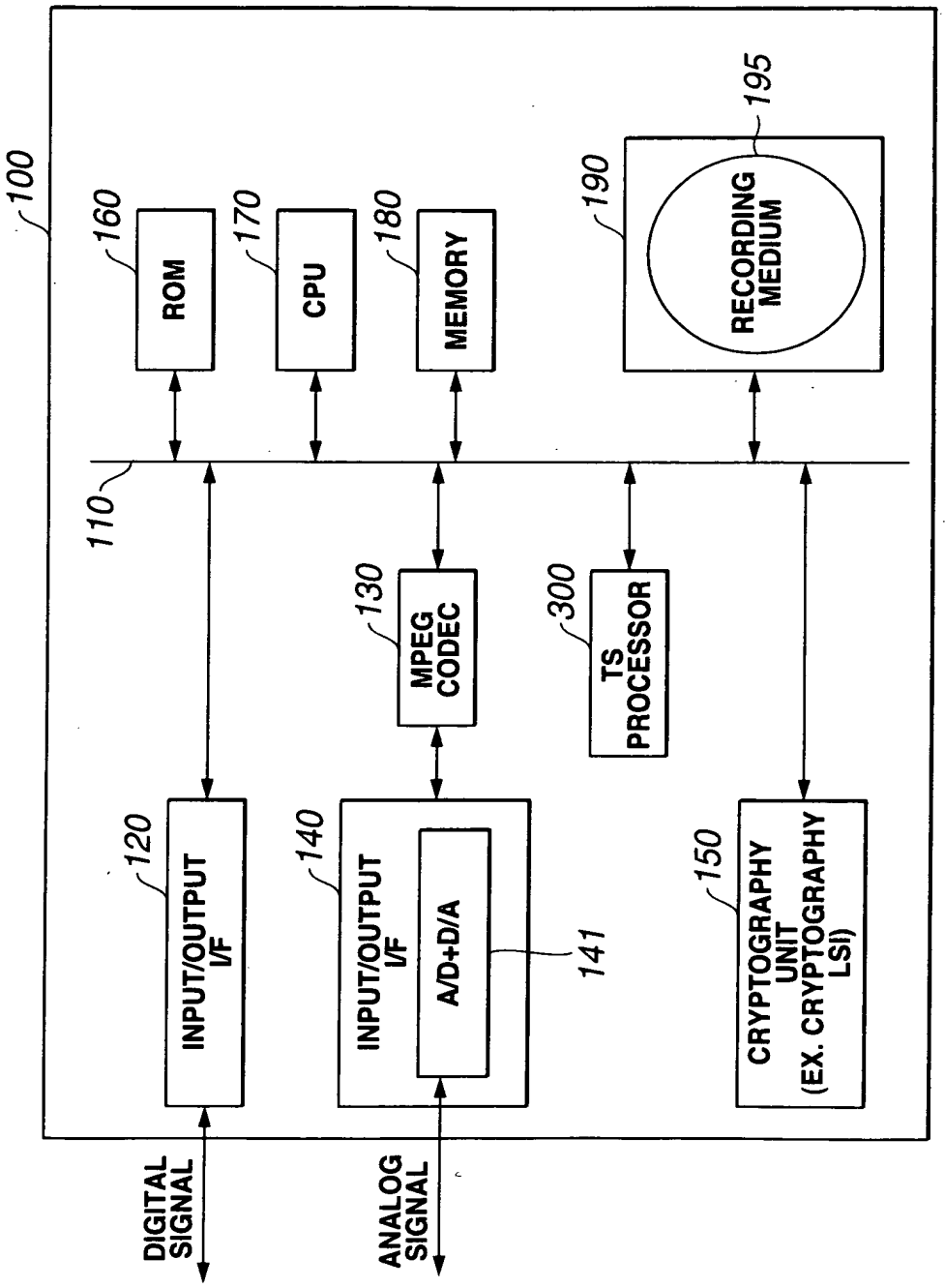


FIG.1

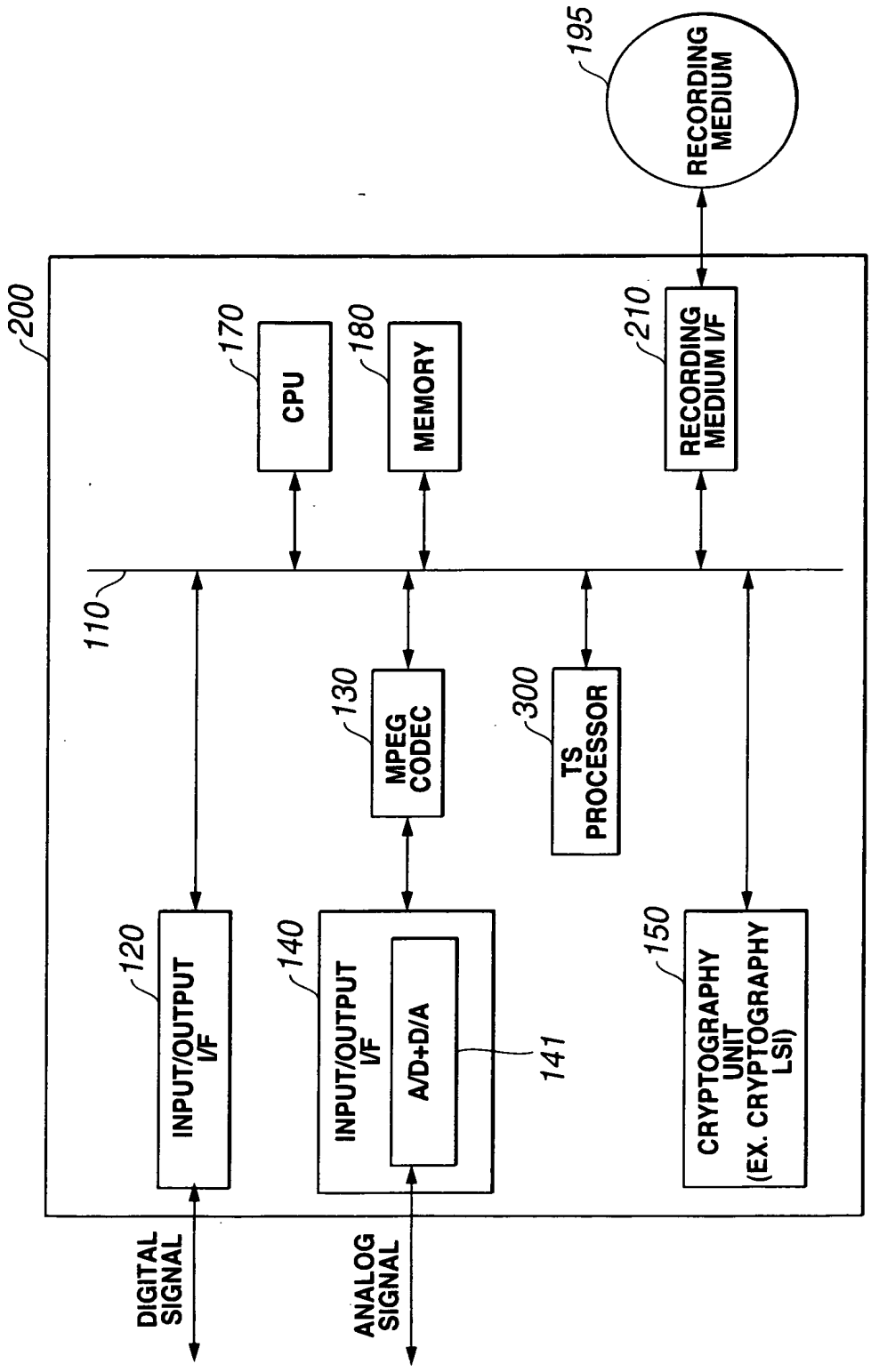

195
RECORDING MEDIUM
200
170
CPU
180
MEMORY
210
RECORDING MEDIUM I/F
110
130
MPEG CODEC
300
TS PROCESSOR
120
INPUT/OUTPUT I/F
140
INPUT/OUTPUT I/F
A/D+D/A
141
150
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
DIGITAL SIGNAL
ANALOG SIGNAL

FIG.2

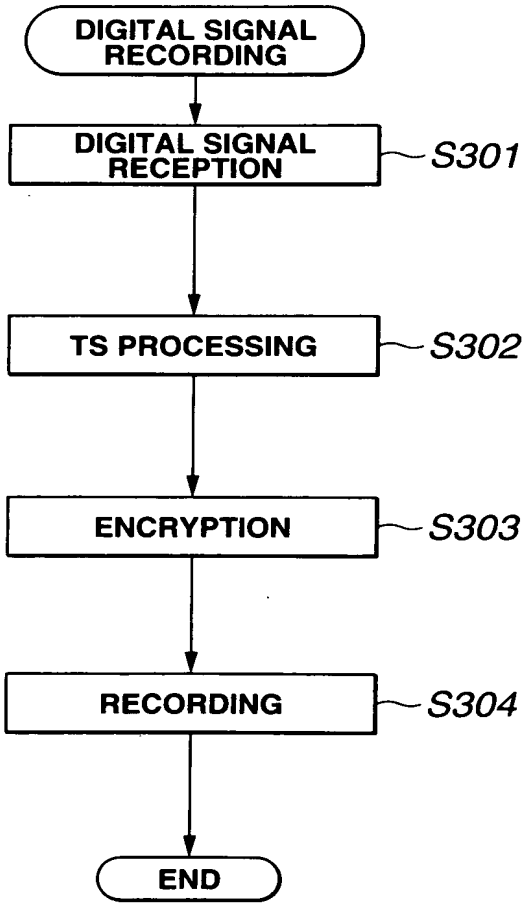

DIGITAL SIGNAL RECORDING
DIGITAL SIGNAL RECEPTION
S301
TS PROCESSING
S302
ENCRYPTION
S303
RECORDING
S304
END

FIG.3A

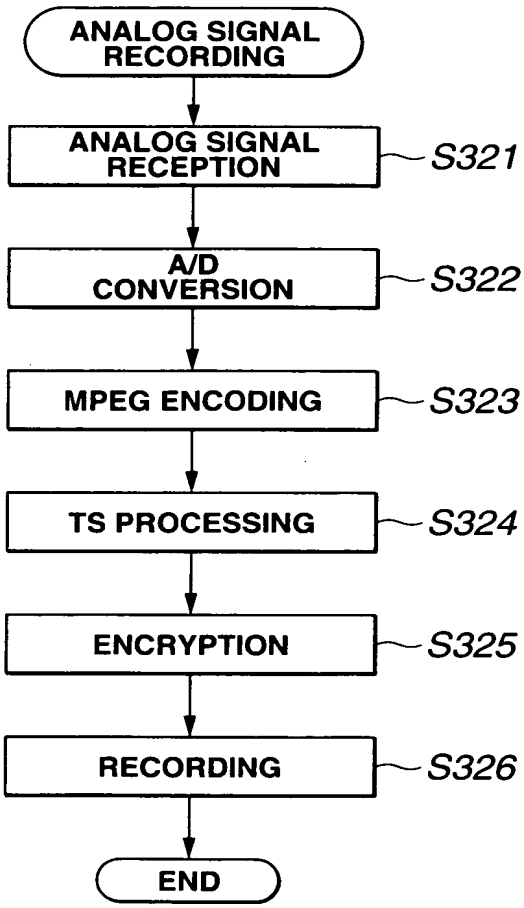

ANALOG SIGNAL RECORDING
ANALOG SIGNAL RECEPTION
S321
A/D CONVERSION
S322
MPEG ENCODING
S323
TS PROCESSING
S324
ENCRYPTION
S325
RECORDING
S326
END

FIG.3B

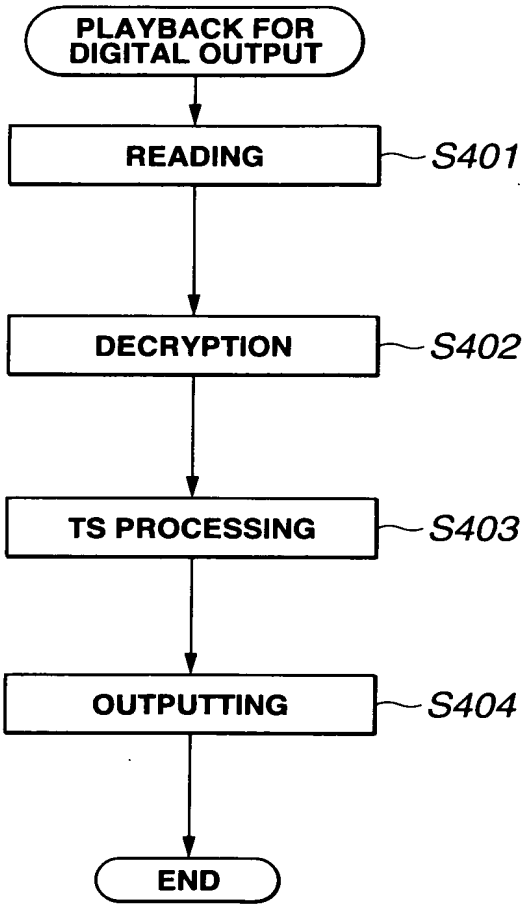

PLAYBACK FOR DIGITAL OUTPUT
READING
S401
DECRYPTION
S402
TS PROCESSING
S403
OUTPUTTING
S404
END

FIG.4A

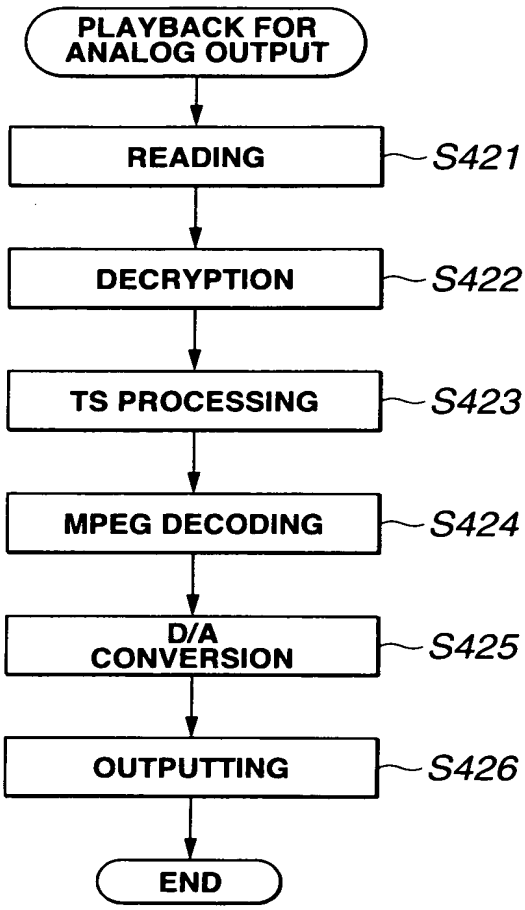

PLAYBACK FOR ANALOG OUTPUT
READING
S421
DECRYPTION
S422
TS PROCESSING
S423
MPEG DECODING
S424
D/A CONVERSION
S425
OUTPUTTING
S426
END

FIG.4B

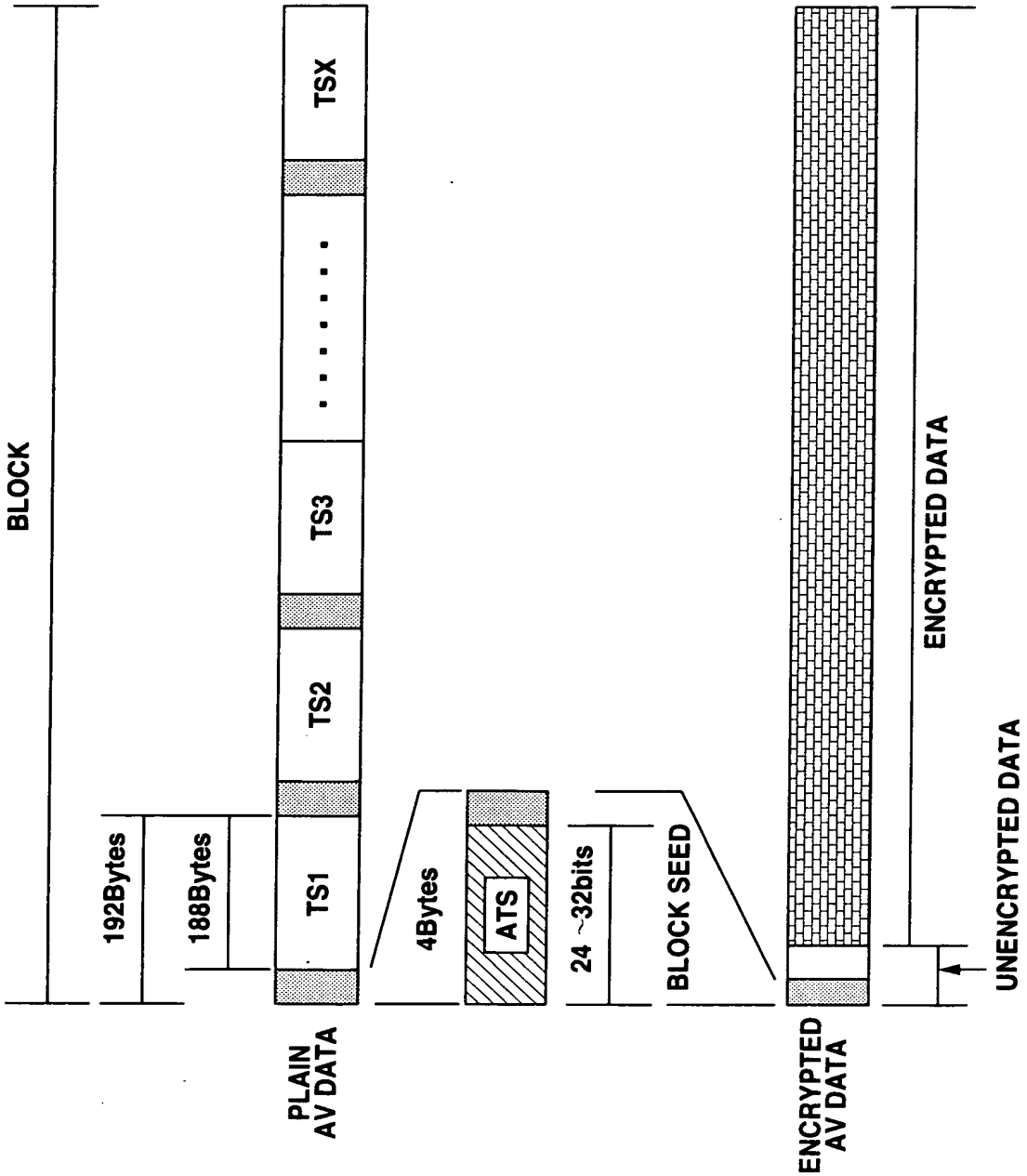

BLOCK
192Bytes
188Bytes
TS1
TS2
TS3
TSX
PLAIN AV DATA
4Bytes
ATS
24 ~32bits
BLOCK SEED
ENCRYPTED AV DATA
ENCRYPTED DATA
UNENCRYPTED DATA

FIG.5

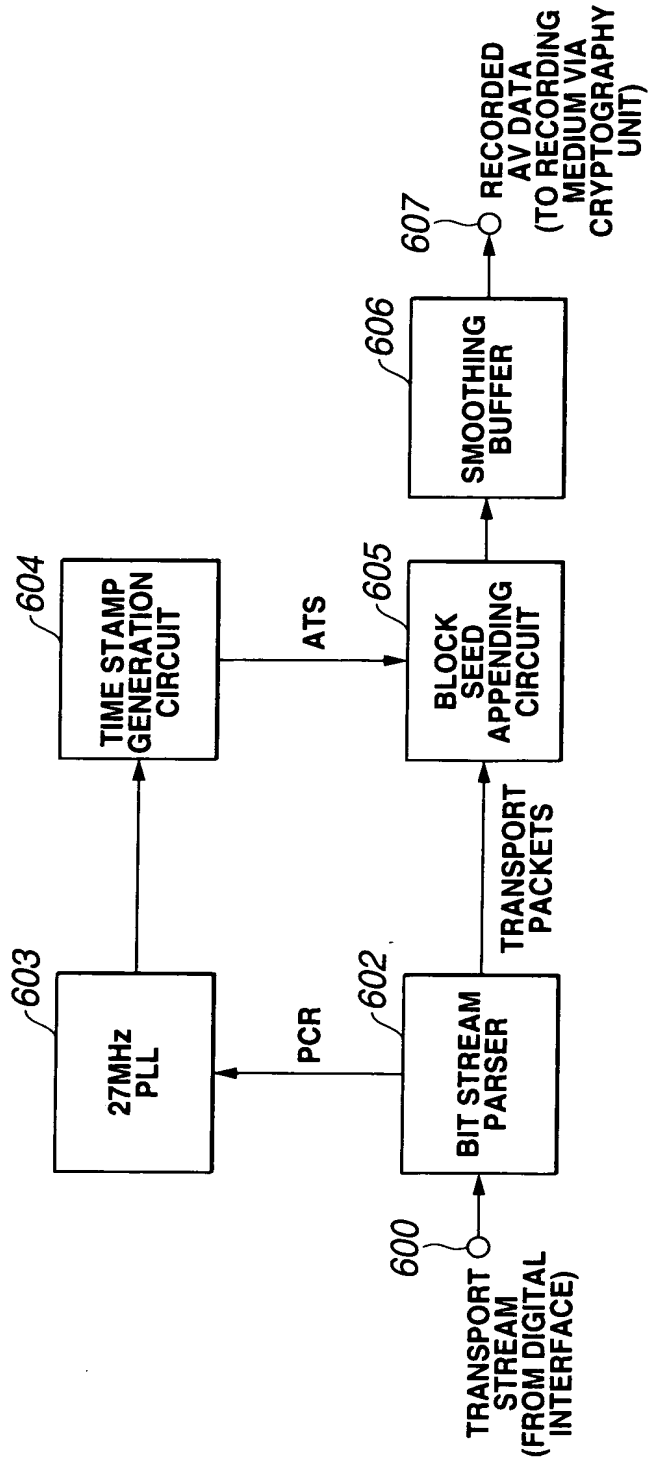

600
TRANSPORT STREAM (FROM DIGITAL INTERFACE)
602
BIT STREAM PARSER
603
27MHz PLL
604
TIME STAMP GENERATION CIRCUIT
605
BLOCK SEED APPENDING CIRCUIT
606
SMOOTHING BUFFER
607
RECORDED AV DATA (TO RECORDING MEDIUM VIA CRYPTOGRAPHY UNIT)
PCR
ATS
TRANSPORT PACKETS

FIG.6

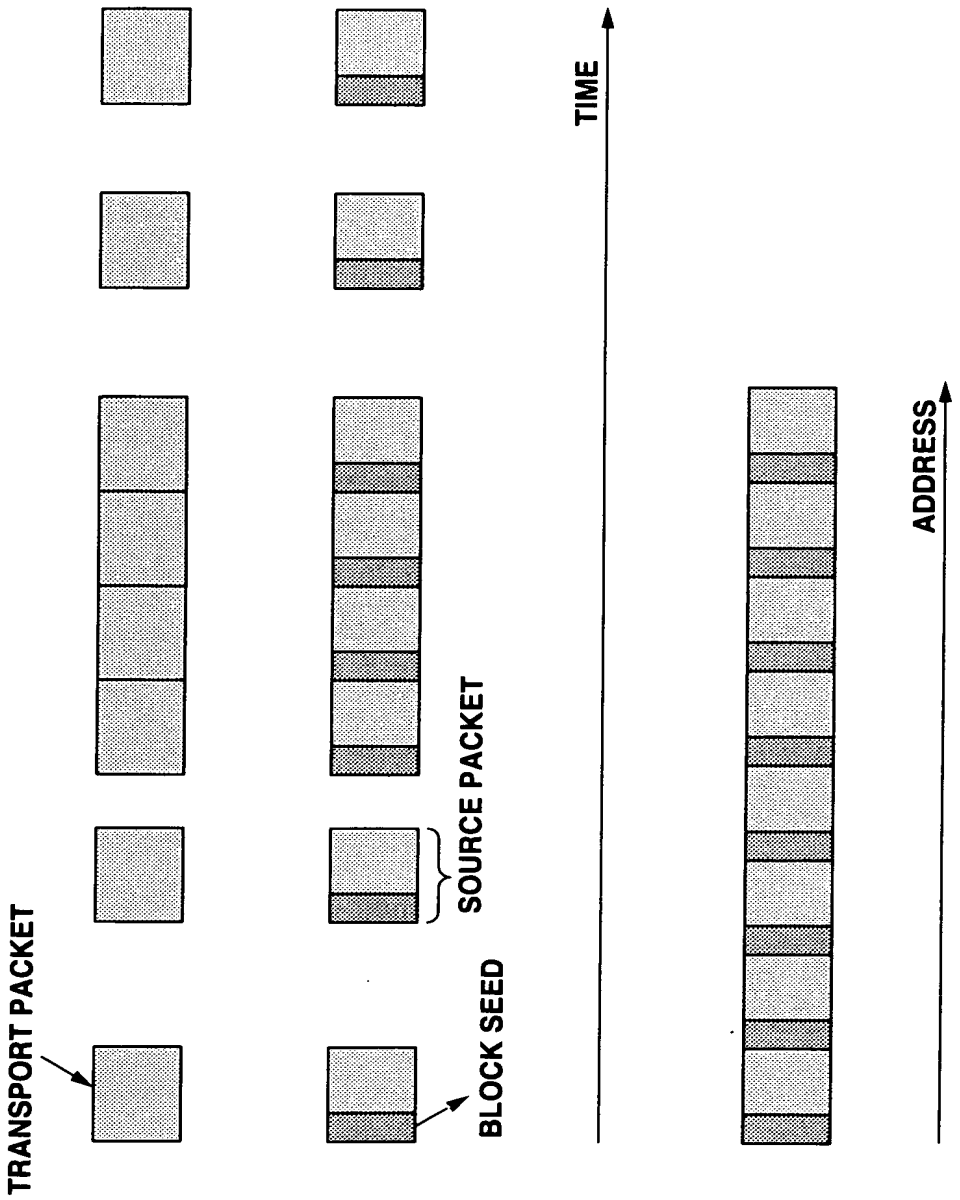


FIG.7A
INPUT TRANSPORT STREAM

FIG.7B
OUTPUT OF BLOCK SEED APPENDING CIRCUIT

FIG.7C
AV DATA ON RECORDING MEDIUM

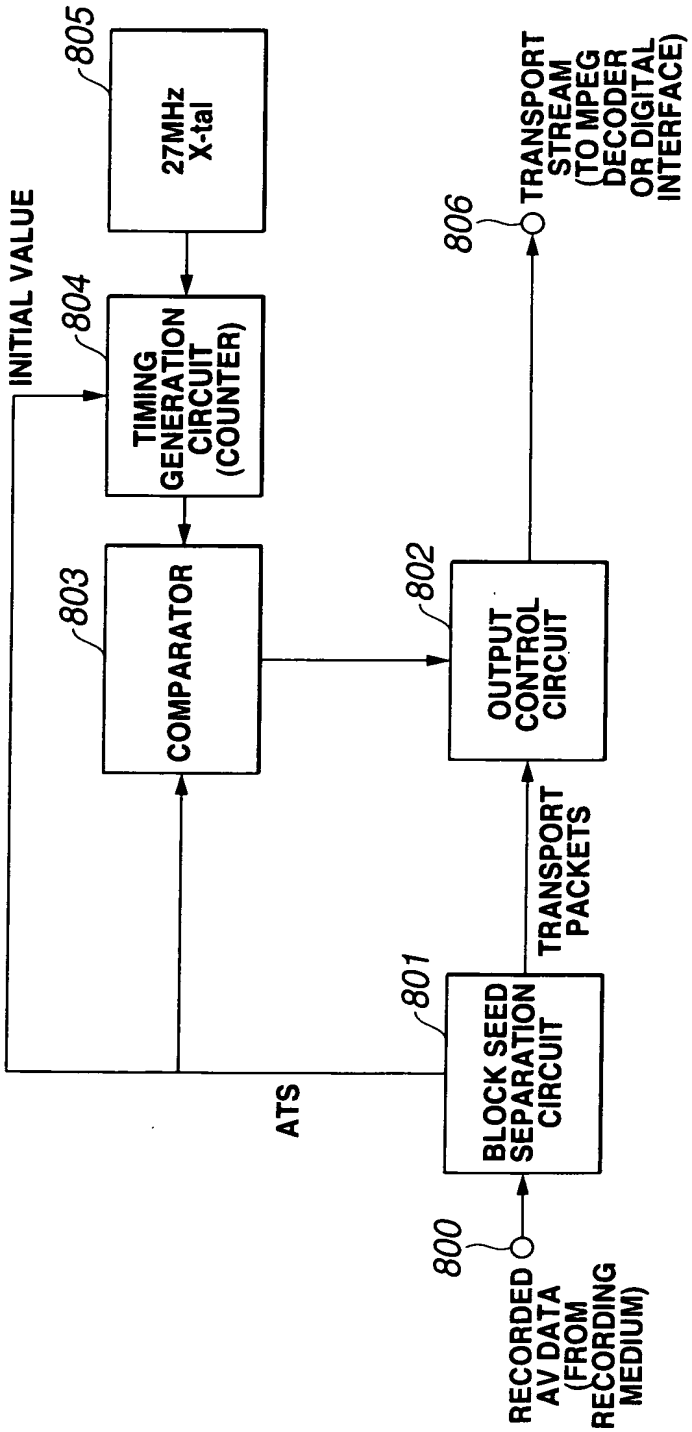

805
27MHz X-tal
804
TIMING GENERATION CIRCUIT (COUNTER)
INITIAL VALUE
803
COMPARATOR
802
OUTPUT CONTROL CIRCUIT
806
TRANSPORT STREAM (TO MPEG DECODER OR DIGITAL INTERFACE)
801
BLOCK SEED SEPARATION CIRCUIT
TRANSPORT PACKETS
ATS
800
RECORDED AV DATA (FROM RECORDING MEDIUM)

FIG.8

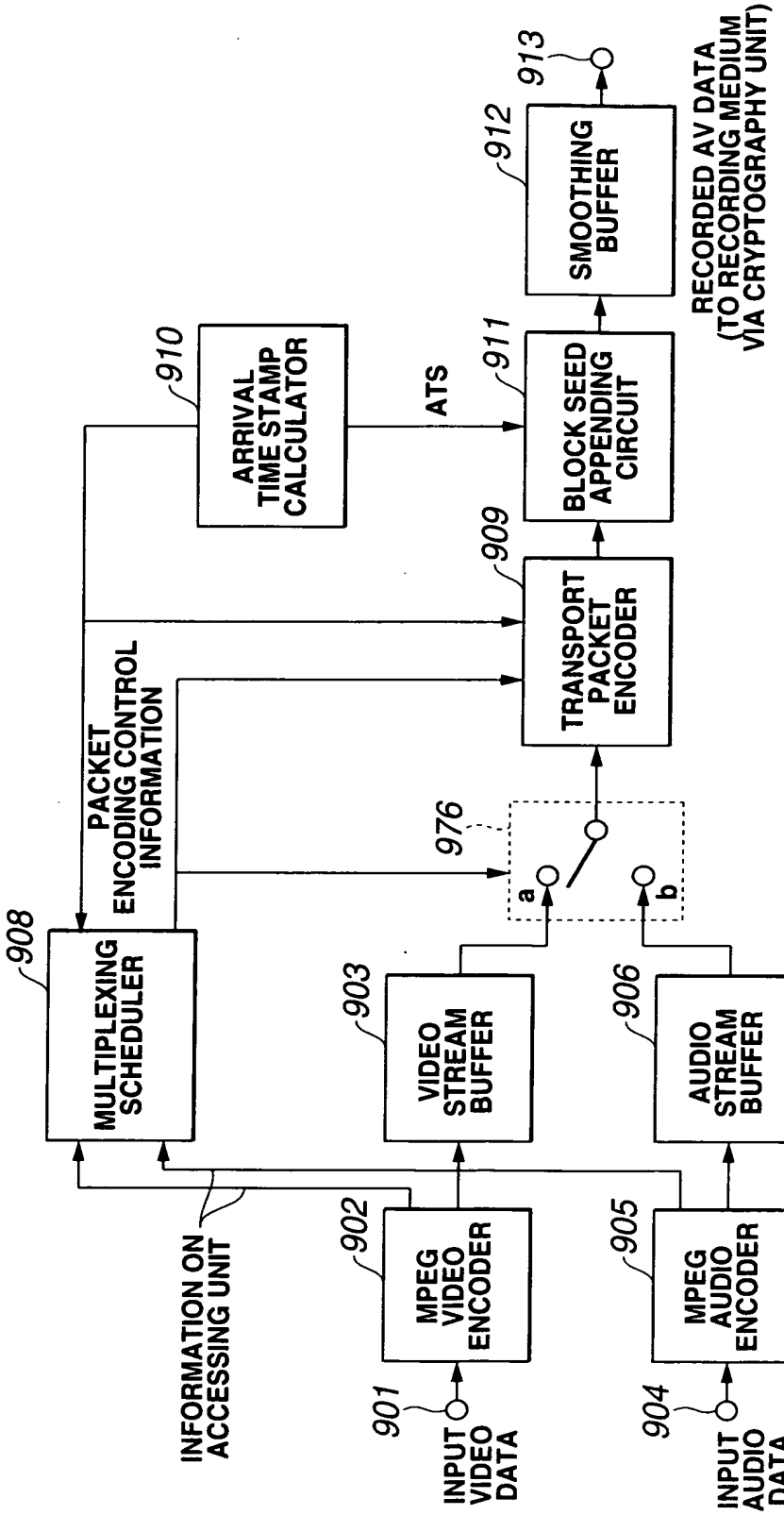

INPUT VIDEO DATA
901
MPEG VIDEO ENCODER
902
INPUT AUDIO DATA
904
MPEG AUDIO ENCODER
905
VIDEO STREAM BUFFER
903
AUDIO STREAM BUFFER
906
INFORMATION ON ACCESSING UNIT
MULTIPLEXING SCHEDULER
908
PACKET ENCODING CONTROL INFORMATION
976
a
b
TRANSPORT PACKET ENCODER
909
ARRIVAL TIME STAMP CALCULATOR
910
ATS
BLOCK SEED APPENDING CIRCUIT
911
SMOOTHING BUFFER
912
913
RECORDED AV DATA (TO RECORDING MEDIUM VIA CRYPTOGRAPHY UNIT)

FIG.9

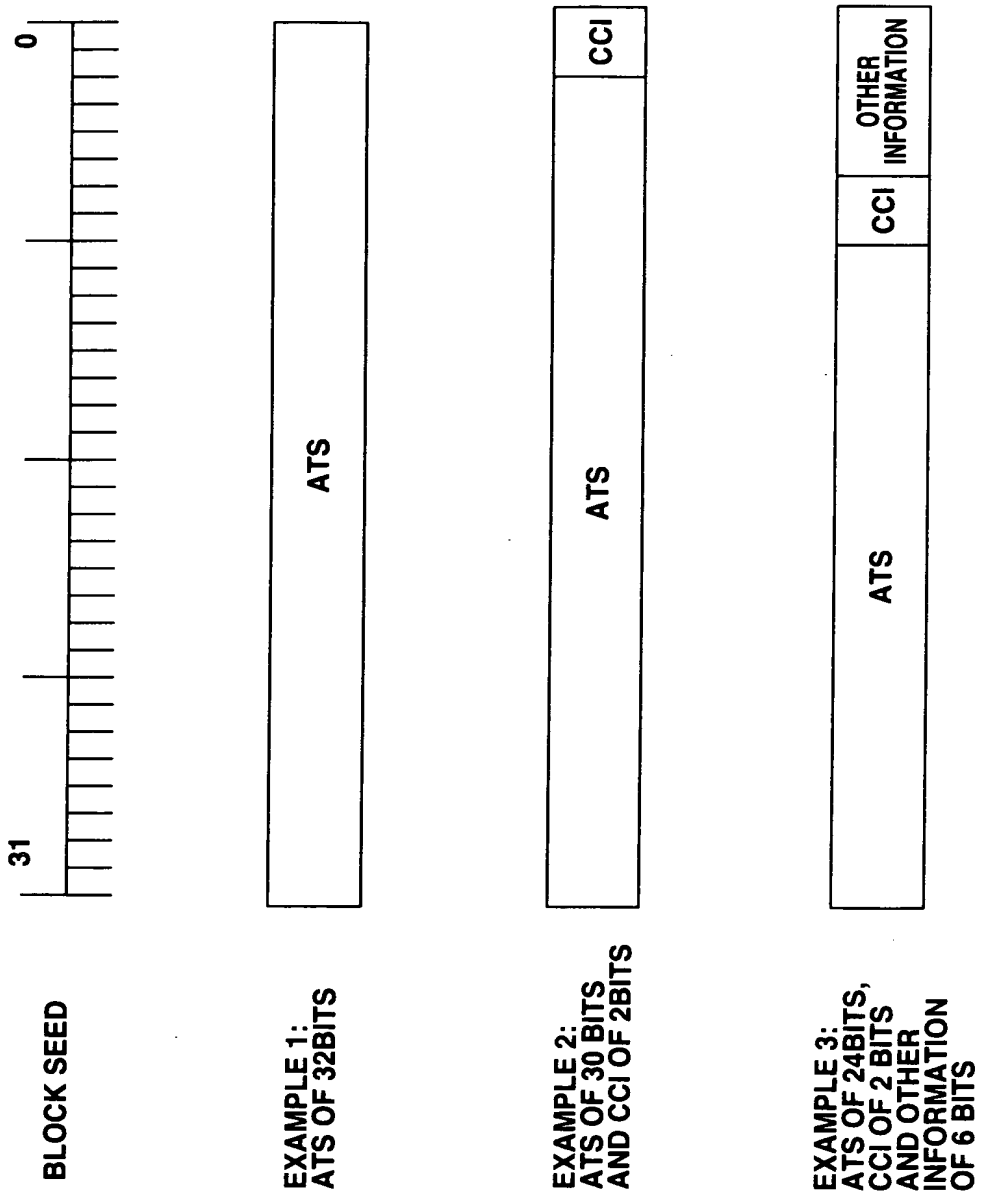

0
31
BLOCK SEED
ATS
EXAMPLE 1:
ATS OF 32BITS
ATS
CCI
EXAMPLE 2:
ATS OF 30 BITS
AND CCI OF 2BITS
ATS
CCI
OTHER INFORMATION
EXAMPLE 3:
ATS OF 24BITS,
CCI OF 2 BITS
AND OTHER
INFORMATION
OF 6 BITS

FIG.10

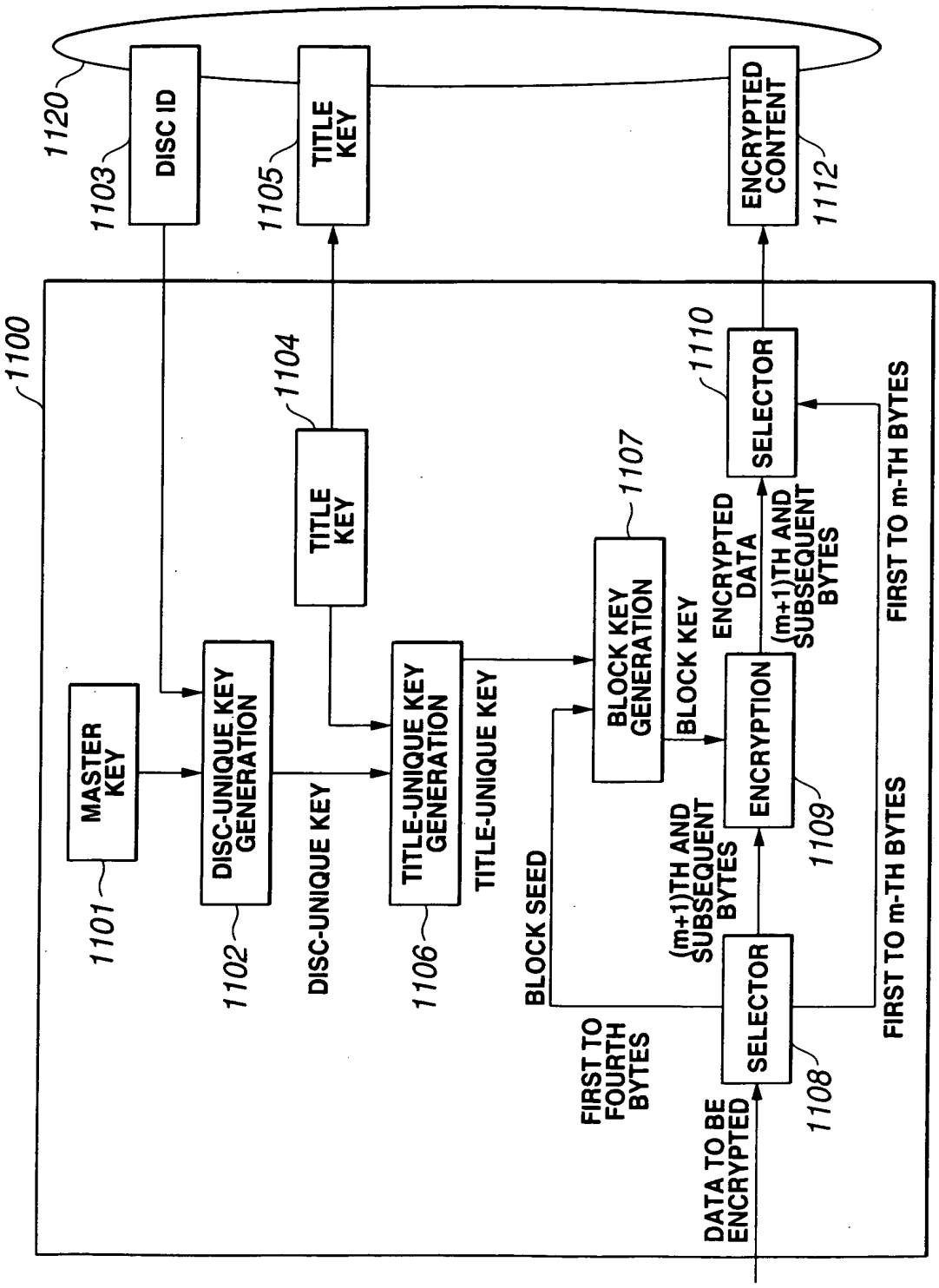

1120
DISC ID
1103
TITLE KEY
1105
ENCRYPTED CONTENT
1112
1100
1104
TITLE KEY
1110
SELECTOR
1107
BLOCK KEY GENERATION
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
MASTER KEY
1101
DISC-UNIQUE KEY GENERATION
1102
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
1106
TITLE-UNIQUE KEY
BLOCK KEY
ENCRYPTION
1109
BLOCK SEED
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO FOURTH BYTES
SELECTOR
1108
FIRST TO m-TH BYTES
DATA TO BE ENCRYPTED

FIG.11

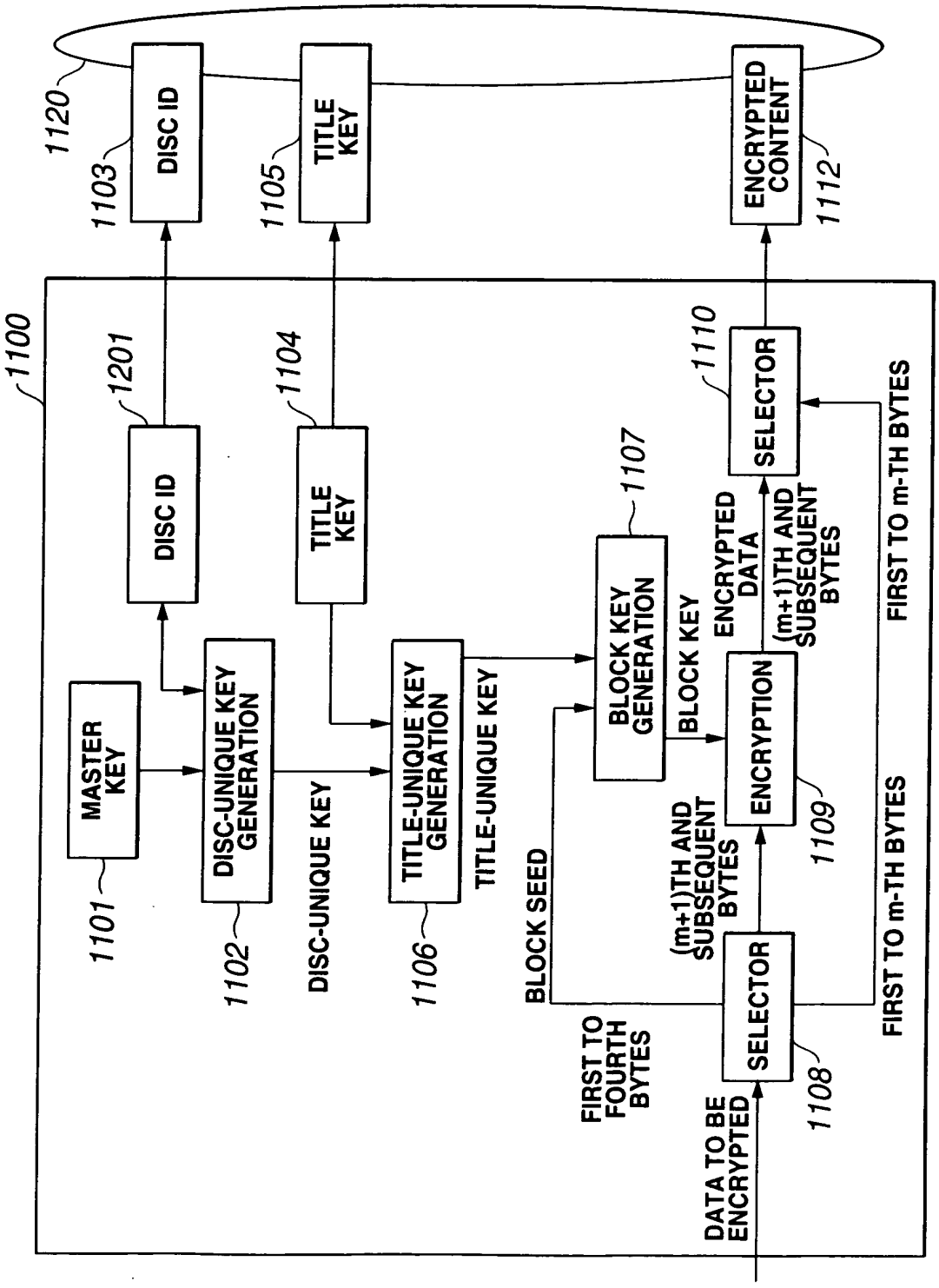

1120
1103
DISC ID
1105
TITLE KEY
ENCRYPTED CONTENT
1112
1100
1201
DISC ID
1104
TITLE KEY
1110
SELECTOR
1107
BLOCK KEY GENERATION
MASTER KEY
1101
DISC-UNIQUE KEY GENERATION
1102
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
1106
TITLE-UNIQUE KEY
BLOCK KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
ENCRYPTION
1109
BLOCK SEED
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
FIRST TO FOURTH BYTES
SELECTOR
1108
DATA TO BE ENCRYPTED
FIRST TO m-TH BYTES

FIG.12

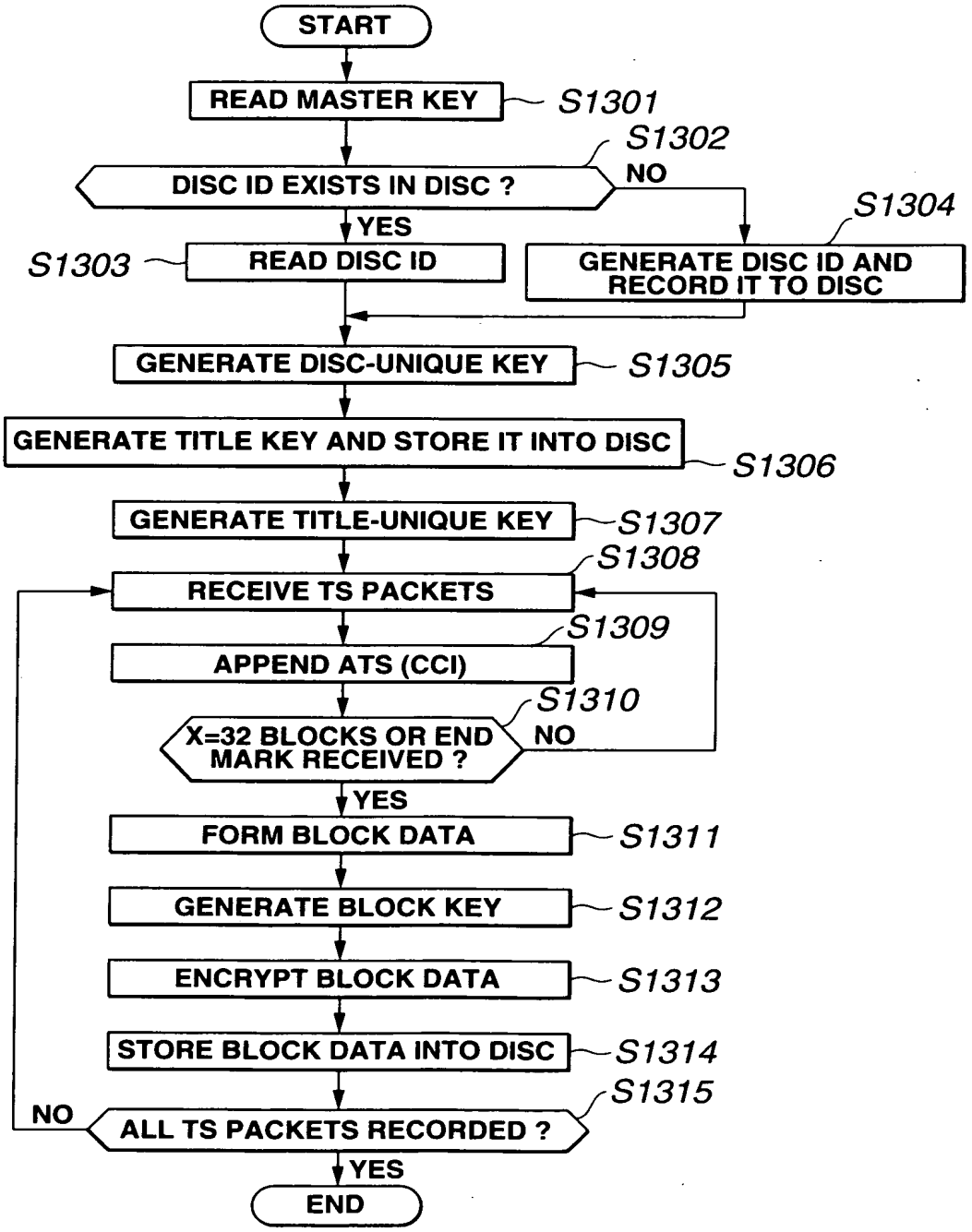
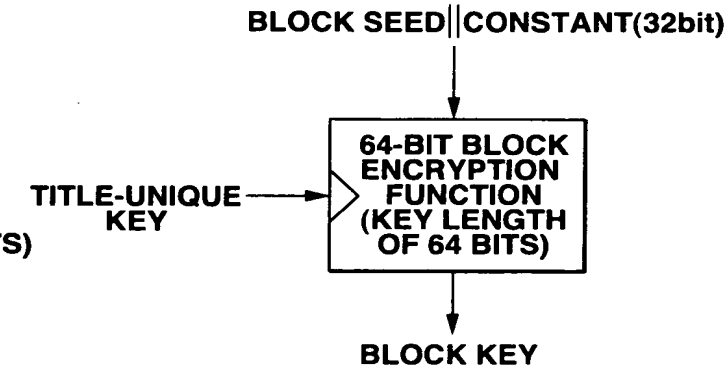

START
READ MASTER KEY
S1301
S1302
DISC ID EXISTS IN DISC ?
NO
YES
S1304
S1303
READ DISC ID
GENERATE DISC ID AND RECORD IT TO DISC
GENERATE DISC-UNIQUE KEY
S1305
GENERATE TITLE KEY AND STORE IT INTO DISC
S1306
GENERATE TITLE-UNIQUE KEY
S1307
S1308
RECEIVE TS PACKETS
S1309
APPEND ATS (CCI)
S1310
X=32 BLOCKS OR END MARK RECEIVED ?
NO
YES
FORM BLOCK DATA
S1311
GENERATE BLOCK KEY
S1312
ENCRYPT BLOCK DATA
S1313
STORE BLOCK DATA INTO DISC
S1314
S1315
NO
ALL TS PACKETS RECORDED ?
YES
END

FIG.13

EXAMPLE 1

EXAMPLE OF BLOCK KEY GENERATION

INPUTS:
BLOCK SEED (32BITS)
TITLE-UNIQUE KEY (64BITS)



EXAMPLE 2

OUTPUTS:
BLOCK KEY (64BITS)

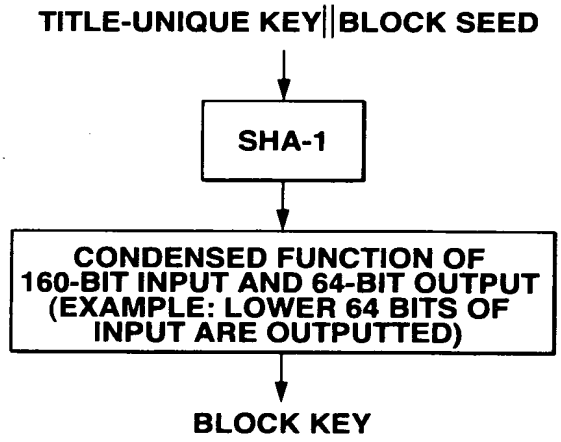


FIG.14

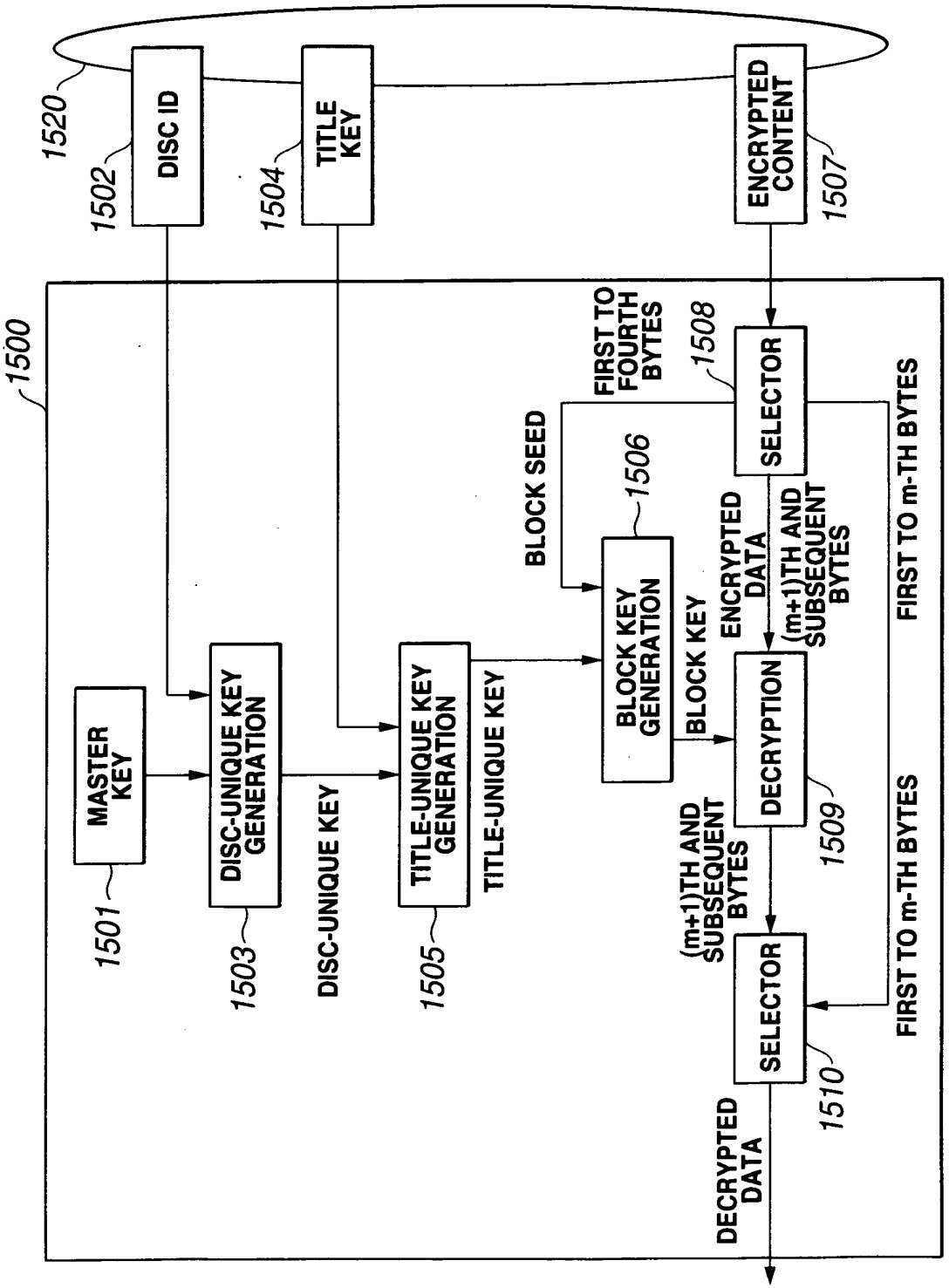

1520
1502
DISC ID
1504
TITLE KEY
ENCRYPTED CONTENT
1507
1500
FIRST TO FOURTH BYTES
1508
SELECTOR
BLOCK SEED
1506
BLOCK KEY GENERATION
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
MASTER KEY
1501
DISC-UNIQUE KEY GENERATION
1503
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
1505
TITLE-UNIQUE KEY
BLOCK KEY
DECRYPTION
1509
(m+1)TH AND SUBSEQUENT BYTES
SELECTOR
1510
FIRST TO m-TH BYTES
DECRYPTED DATA

FIG.15

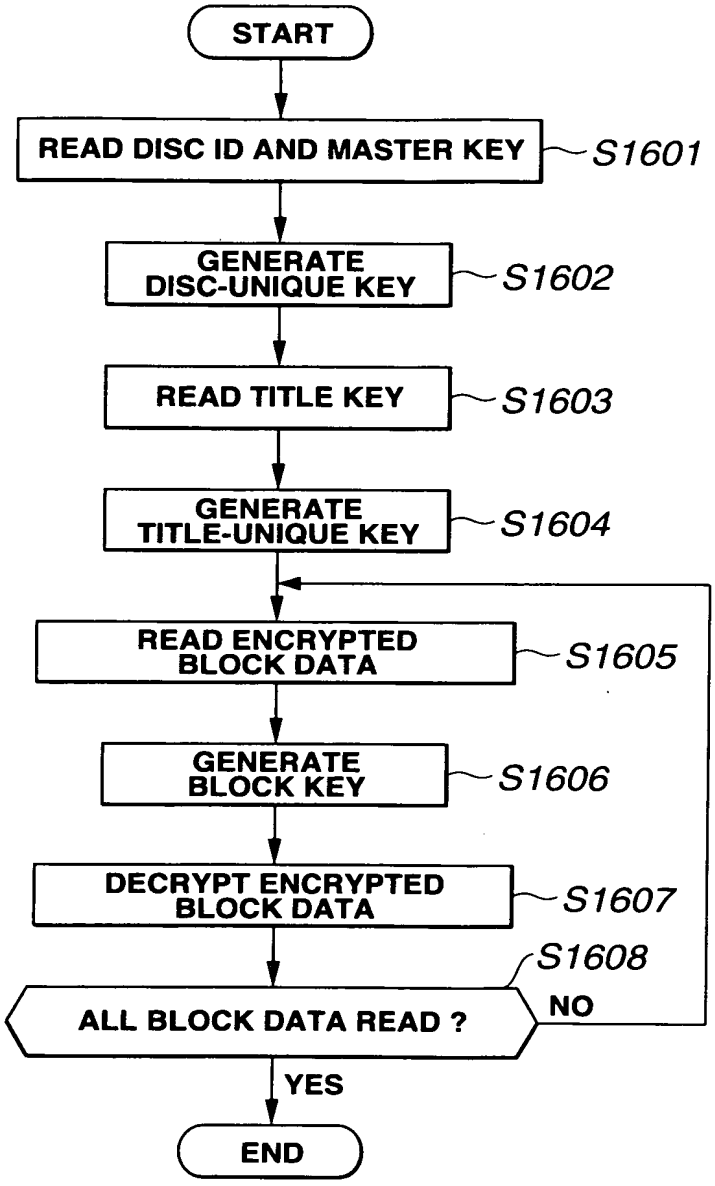

START
READ DISC ID AND MASTER KEY
S1601
GENERATE DISC-UNIQUE KEY
S1602
READ TITLE KEY
S1603
GENERATE TITLE-UNIQUE KEY
S1604
READ ENCRYPTED BLOCK DATA
S1605
GENERATE BLOCK KEY
S1606
DECRYPT ENCRYPTED BLOCK DATA
S1607
S1608
ALL BLOCK DATA READ ?
NO
YES
END

FIG.16

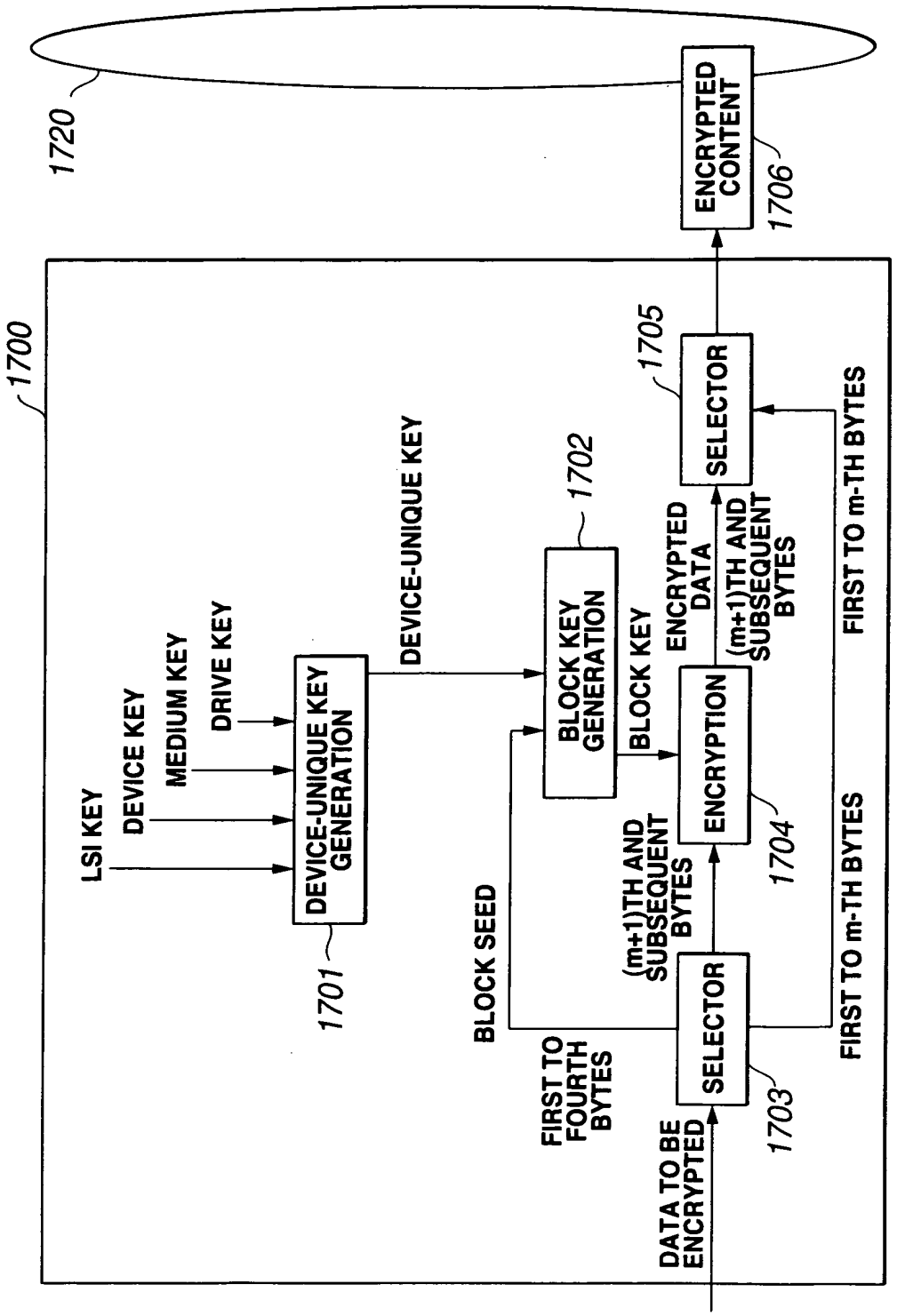

1720
ENCRYPTED CONTENT
1706
1700
1705
SELECTOR
FIRST TO m-TH BYTES
1702
BLOCK KEY GENERATION
DEVICE-UNIQUE KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
LSI KEY
DEVICE KEY
MEDIUM KEY
DRIVE KEY
DEVICE-UNIQUE KEY GENERATION
1701
BLOCK KEY
ENCRYPTION
1704
BLOCK SEED
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO FOURTH BYTES
SELECTOR
1703
FIRST TO m-TH BYTES
DATA TO BE ENCRYPTED

FIG.17

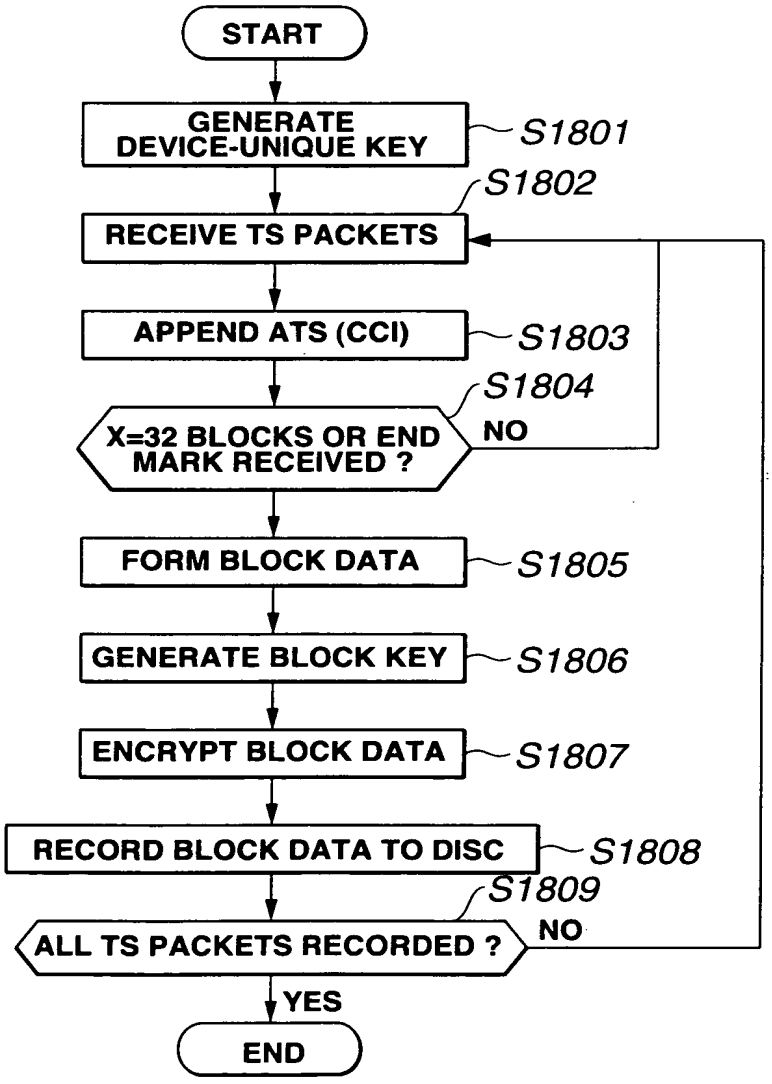

START
GENERATE DEVICE-UNIQUE KEY
S1801
S1802
RECEIVE TS PACKETS
APPEND ATS (CCI)
S1803
S1804
X=32 BLOCKS OR END MARK RECEIVED ?
NO
FORM BLOCK DATA
S1805
GENERATE BLOCK KEY
S1806
ENCRYPT BLOCK DATA
S1807
RECORD BLOCK DATA TO DISC
S1808
S1809
ALL TS PACKETS RECORDED ?
NO
YES
END

FIG.18

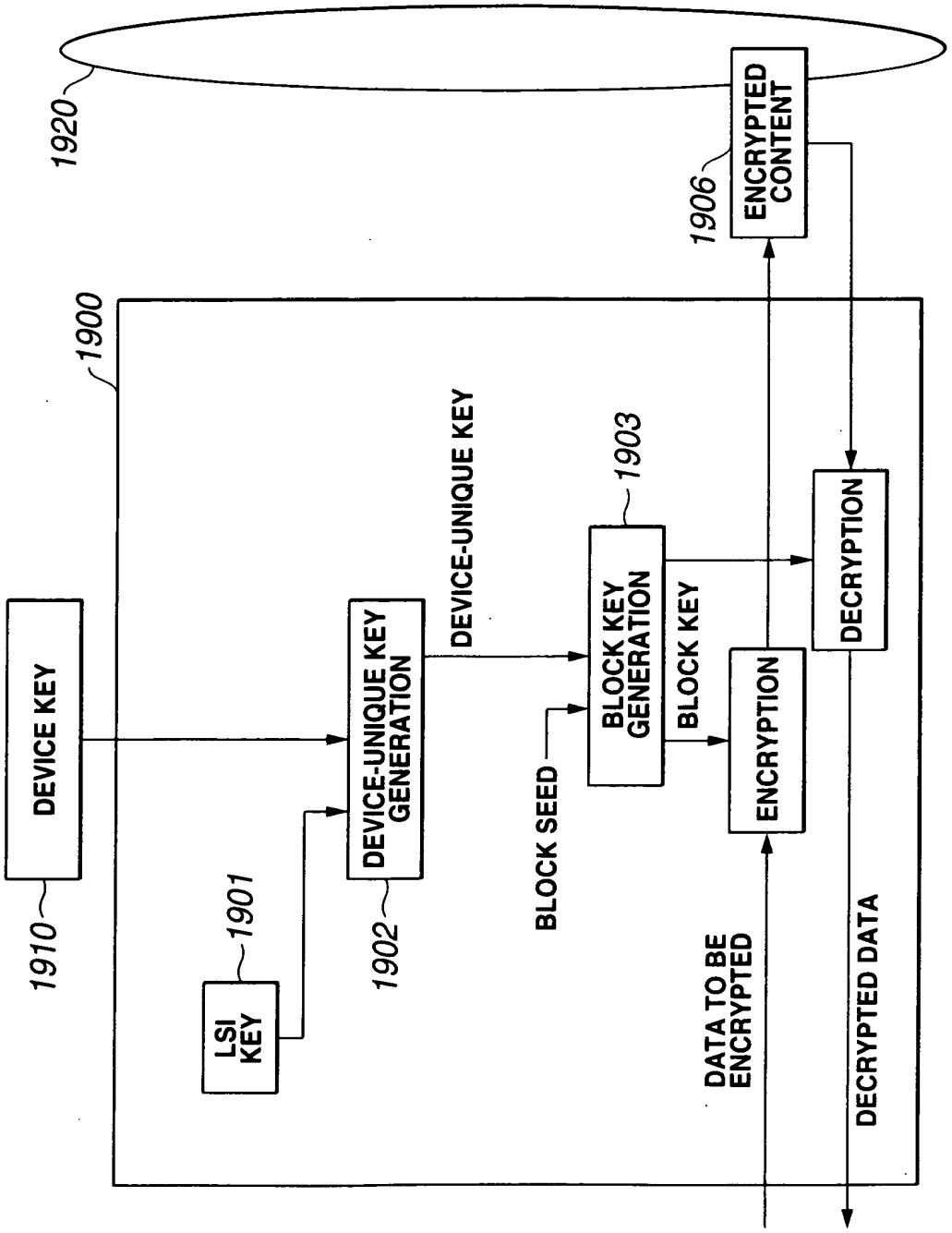

1920
1906
ENCRYPTED CONTENT
1900
DEVICE KEY
1910
LSI KEY
1901
DEVICE-UNIQUE KEY GENERATION
1902
DEVICE-UNIQUE KEY
BLOCK SEED
BLOCK KEY GENERATION
1903
BLOCK KEY
ENCRYPTION
DATA TO BE ENCRYPTED
DECRYPTION
DECRYPTED DATA

FIG.19

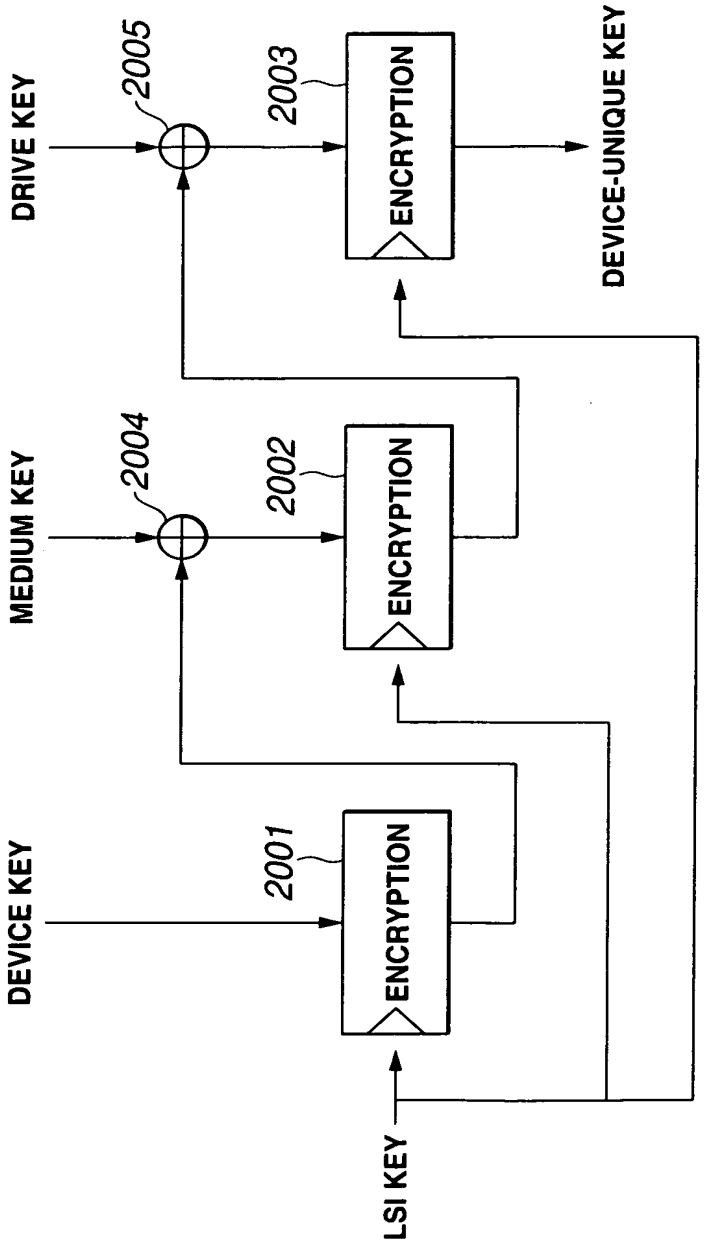

DRIVE KEY
2005
2003
ENCRYPTION
DEVICE-UNIQUE KEY
MEDIUM KEY
2004
2002
ENCRYPTION
DEVICE KEY
2001
ENCRYPTION
LSI KEY

FIG.20

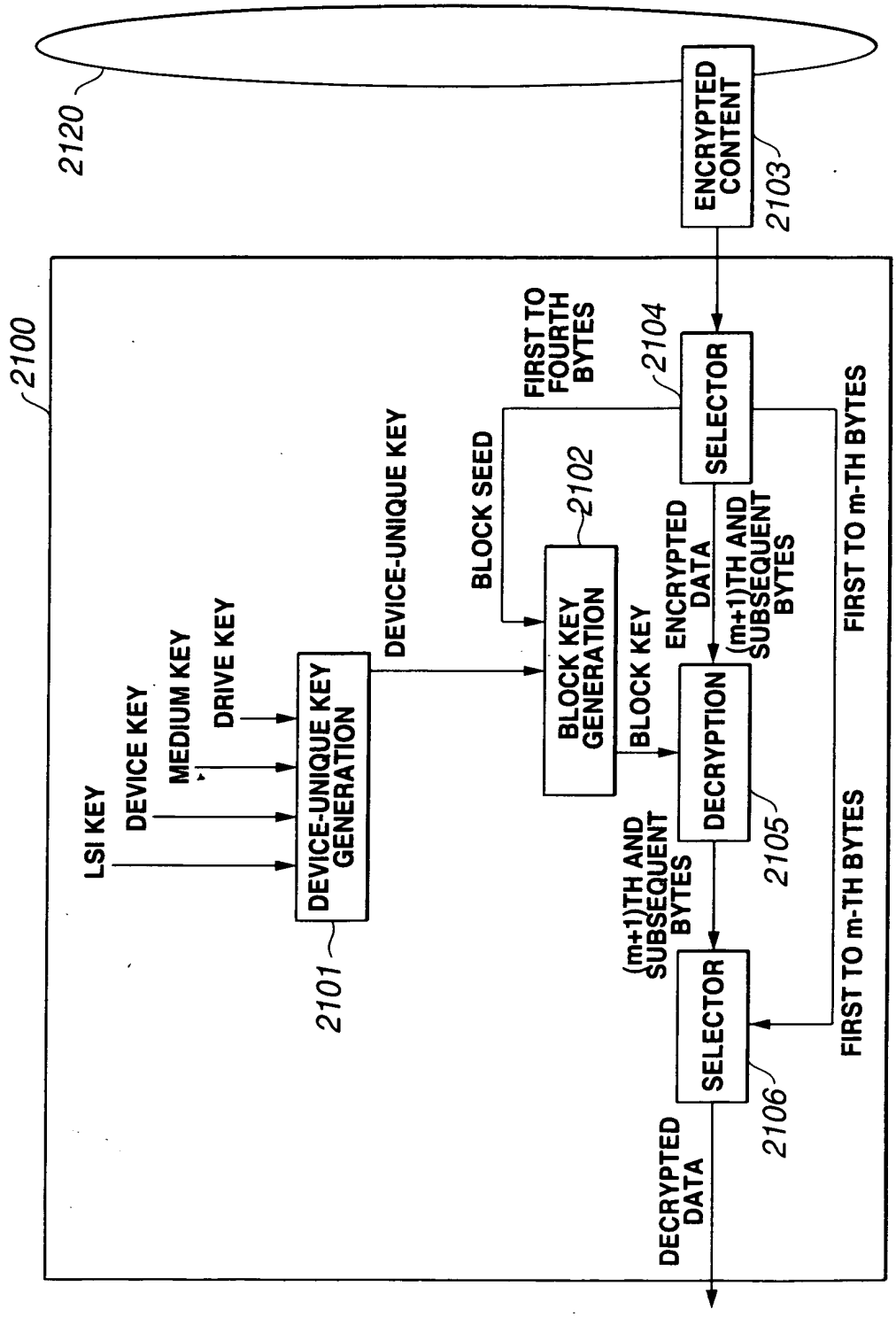

2120
ENCRYPTED CONTENT
2103
2100
FIRST TO FOURTH BYTES
2104
SELECTOR
BLOCK SEED
2102
DEVICE-UNIQUE KEY
LSI KEY
DEVICE KEY
MEDIUM KEY
DRIVE KEY
DEVICE-UNIQUE KEY GENERATION
BLOCK KEY GENERATION
BLOCK KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
2101
DECRYPTION
2105
(m+1)TH AND SUBSEQUENT BYTES
SELECTOR
FIRST TO m-TH BYTES
2106
DECRYPTED DATA

FIG.21

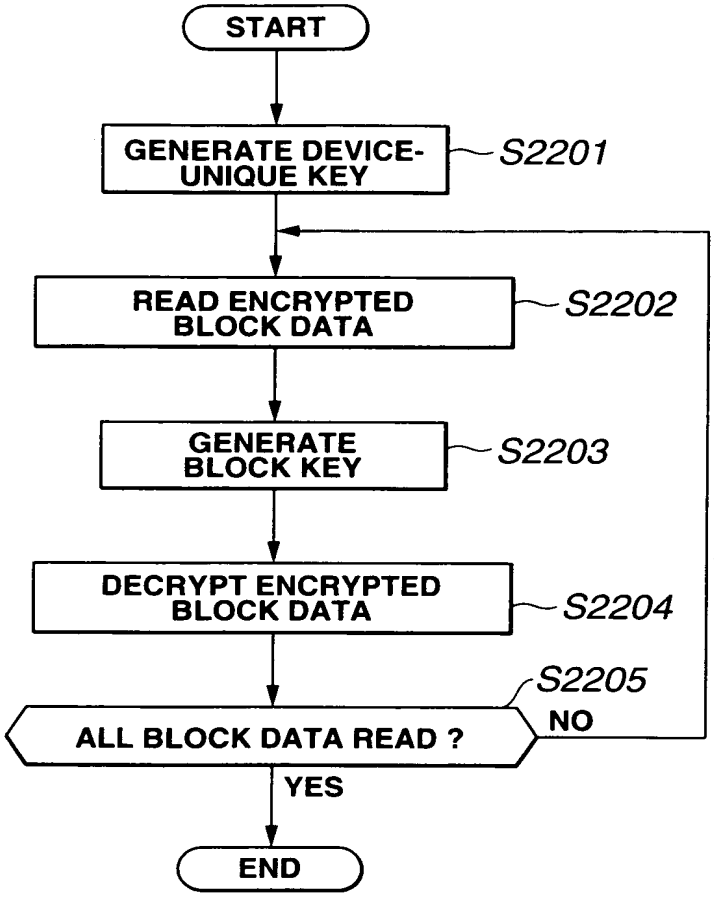

START
GENERATE DEVICE-UNIQUE KEY
S2201
READ ENCRYPTED BLOCK DATA
S2202
GENERATE BLOCK KEY
S2203
DECRYPT ENCRYPTED BLOCK DATA
S2204
S2205
ALL BLOCK DATA READ ?
NO
YES
END

FIG.22

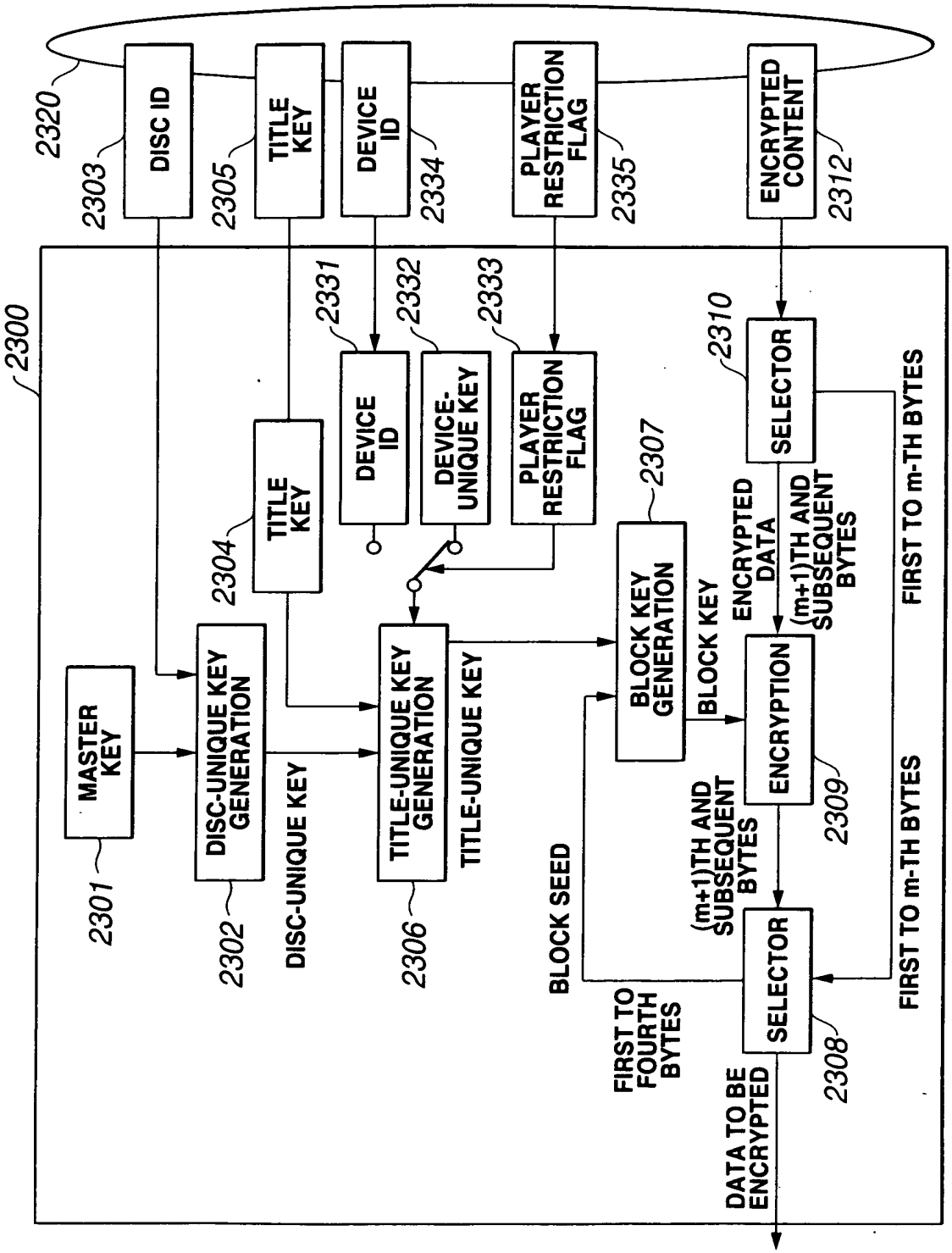

2320
2303
DISC ID
2305
TITLE KEY
2334
DEVICE ID
2335
PLAYER RESTRICTION FLAG
2312
ENCRYPTED CONTENT
2300
2331
DEVICE ID
2332
DEVICE-UNIQUE KEY
2333
PLAYER RESTRICTION FLAG
2310
SELECTOR
2304
TITLE KEY
2307
BLOCK KEY GENERATION
MASTER KEY
2301
DISC-UNIQUE KEY GENERATION
2302
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
2306
TITLE-UNIQUE KEY
BLOCK KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
ENCRYPTION
2309
(m+1)TH AND SUBSEQUENT BYTES
BLOCK SEED
FIRST TO FOURTH BYTES
SELECTOR
2308
DATA TO BE ENCRYPTED

FIG.23

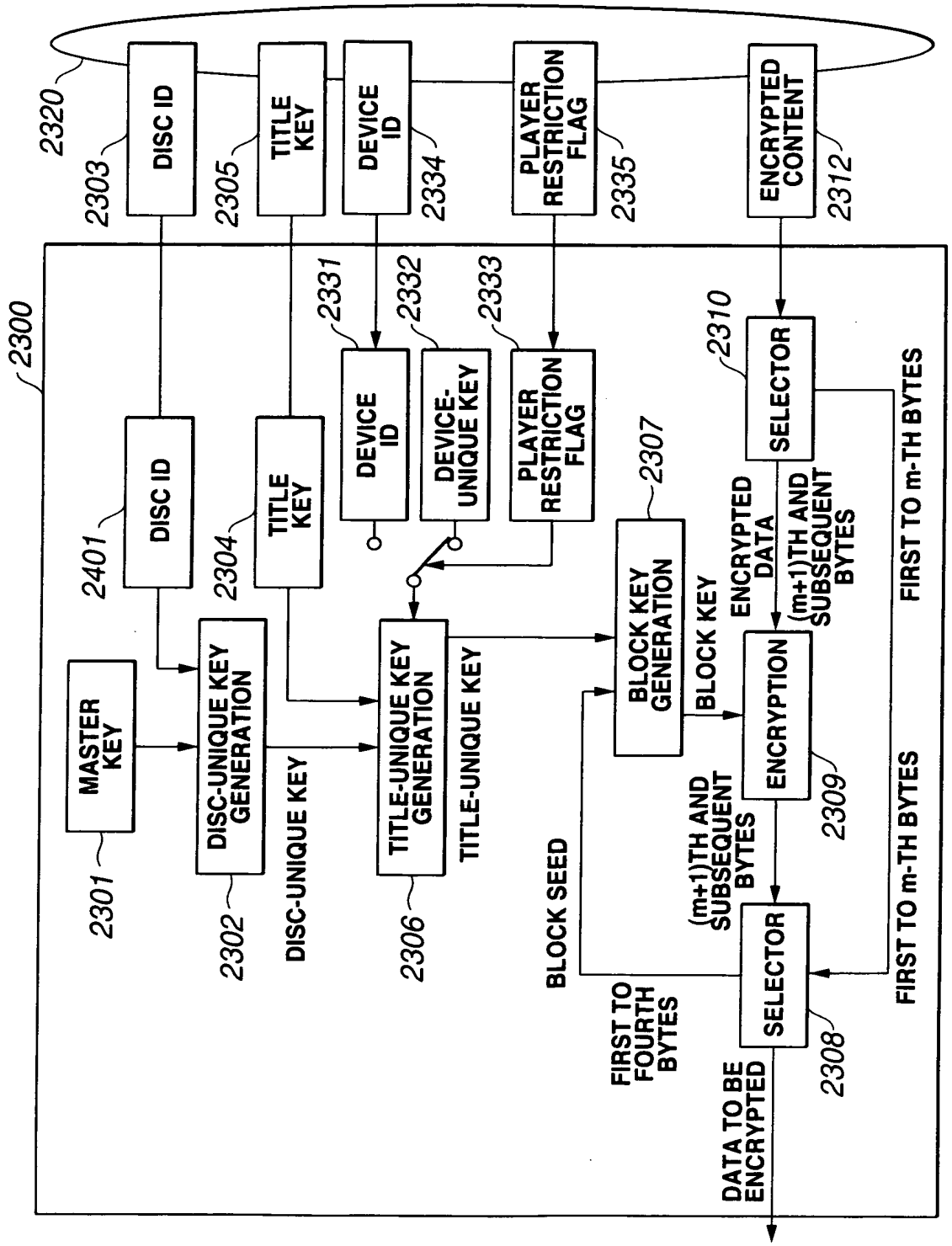

2320
2303
DISC ID
2305
TITLE KEY
2334
DEVICE ID
2335
PLAYER RESTRICTION FLAG
2312
ENCRYPTED CONTENT
2300
2331
2332
2333
2310
SELECTOR
DEVICE ID
DEVICE-UNIQUE KEY
PLAYER RESTRICTION FLAG
2307
2401
DISC ID
2304
TITLE KEY
BLOCK KEY GENERATION
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
MASTER KEY
DISC-UNIQUE KEY GENERATION
TITLE-UNIQUE KEY GENERATION
BLOCK KEY
ENCRYPTION
2309
2301
2302
DISC-UNIQUE KEY
2306
TITLE-UNIQUE KEY
BLOCK SEED
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
FIRST TO FOURTH BYTES
SELECTOR
2308
DATA TO BE ENCRYPTED

FIG.24

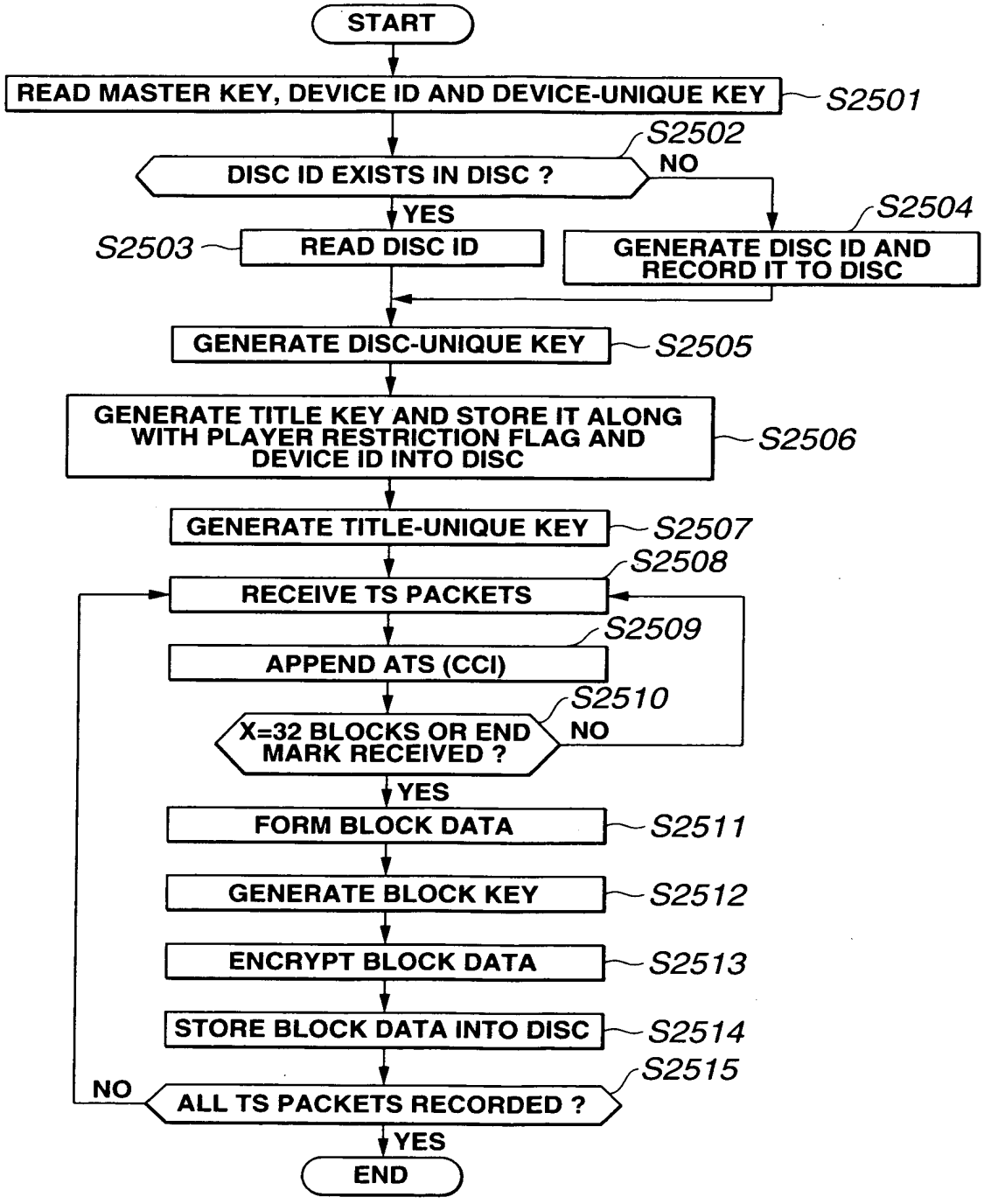
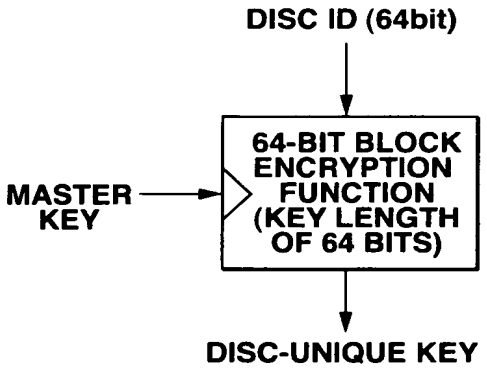

START
READ MASTER KEY, DEVICE ID AND DEVICE-UNIQUE KEY
S2501
S2502
DISC ID EXISTS IN DISC ?
NO
YES
S2503
READ DISC ID
S2504
GENERATE DISC ID AND RECORD IT TO DISC
GENERATE DISC-UNIQUE KEY
S2505
GENERATE TITLE KEY AND STORE IT ALONG WITH PLAYER RESTRICTION FLAG AND DEVICE ID INTO DISC
S2506
GENERATE TITLE-UNIQUE KEY
S2507
S2508
RECEIVE TS PACKETS
S2509
APPEND ATS (CCI)
S2510
X=32 BLOCKS OR END MARK RECEIVED ?
NO
YES
FORM BLOCK DATA
S2511
GENERATE BLOCK KEY
S2512
ENCRYPT BLOCK DATA
S2513
STORE BLOCK DATA INTO DISC
S2514
S2515
NO
ALL TS PACKETS RECORDED ?
YES
END

FIG.25

EXAMPLE 1

EXAMPLE OF DEVICE-UNIQUE KEY GENERATION

INPUTS:
MASTER KEY (64BITS)
DISC ID (64BITS)



EXAMPLE 2

OUTPUTS:
DISC-UNIQUE KEY (64BITS)

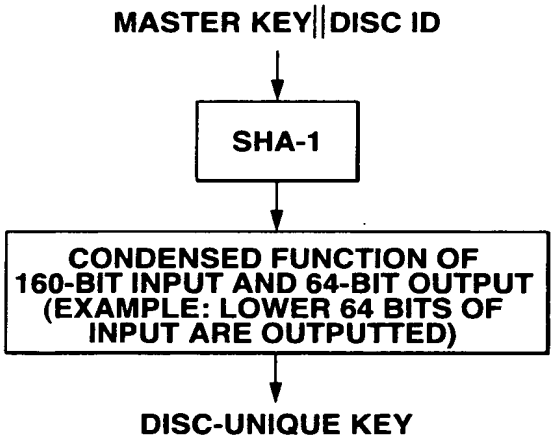


FIG.26

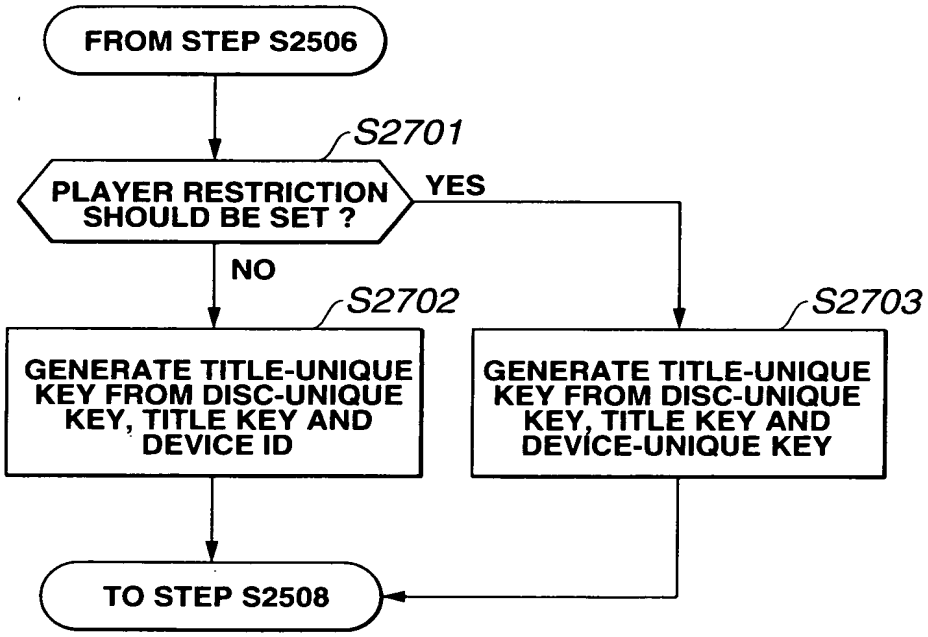

FROM STEP S2506
S2701
PLAYER RESTRICTION SHOULD BE SET ?
YES
NO
S2702
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE ID
S2703
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE-UNIQUE KEY
TO STEP S2508

FIG.27

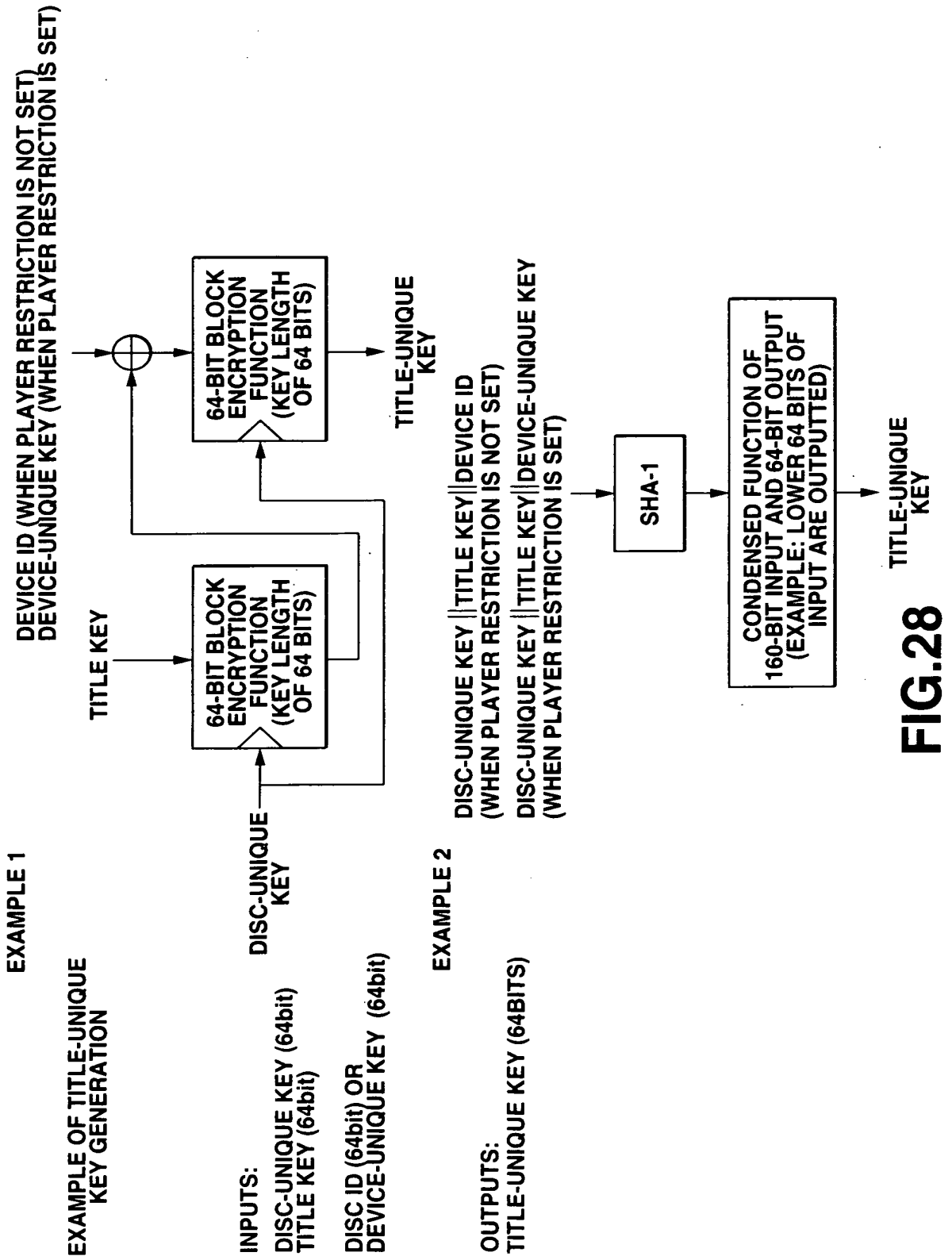

EXAMPLE 1
EXAMPLE OF TITLE-UNIQUE KEY GENERATION
INPUTS:
DISC-UNIQUE KEY (64bit)
TITLE KEY (64bit)
DISC ID (64bit) OR DEVICE-UNIQUE KEY (64bit)
OUTPUTS:
TITLE-UNIQUE KEY (64BITS)
DISC-UNIQUE KEY
TITLE KEY
DEVICE ID (WHEN PLAYER RESTRICTION IS NOT SET)
DEVICE-UNIQUE KEY (WHEN PLAYER RESTRICTION IS SET)
64-BIT BLOCK ENCRYPTION FUNCTION (KEY LENGTH OF 64 BITS)
64-BIT BLOCK ENCRYPTION FUNCTION (KEY LENGTH OF 64 BITS)
TITLE-UNIQUE KEY
EXAMPLE 2
DISC-UNIQUE KEY||TITLE KEY||DEVICE ID (WHEN PLAYER RESTRICTION IS NOT SET)
DISC-UNIQUE KEY||TITLE KEY||DEVICE-UNIQUE KEY (WHEN PLAYER RESTRICTION IS SET)
SHA-1
CONDENSED FUNCTION OF 160-BIT INPUT AND 64-BIT OUTPUT (EXAMPLE: LOWER 64 BITS OF INPUT ARE OUTPUTTED)
TITLE-UNIQUE KEY

FIG.28

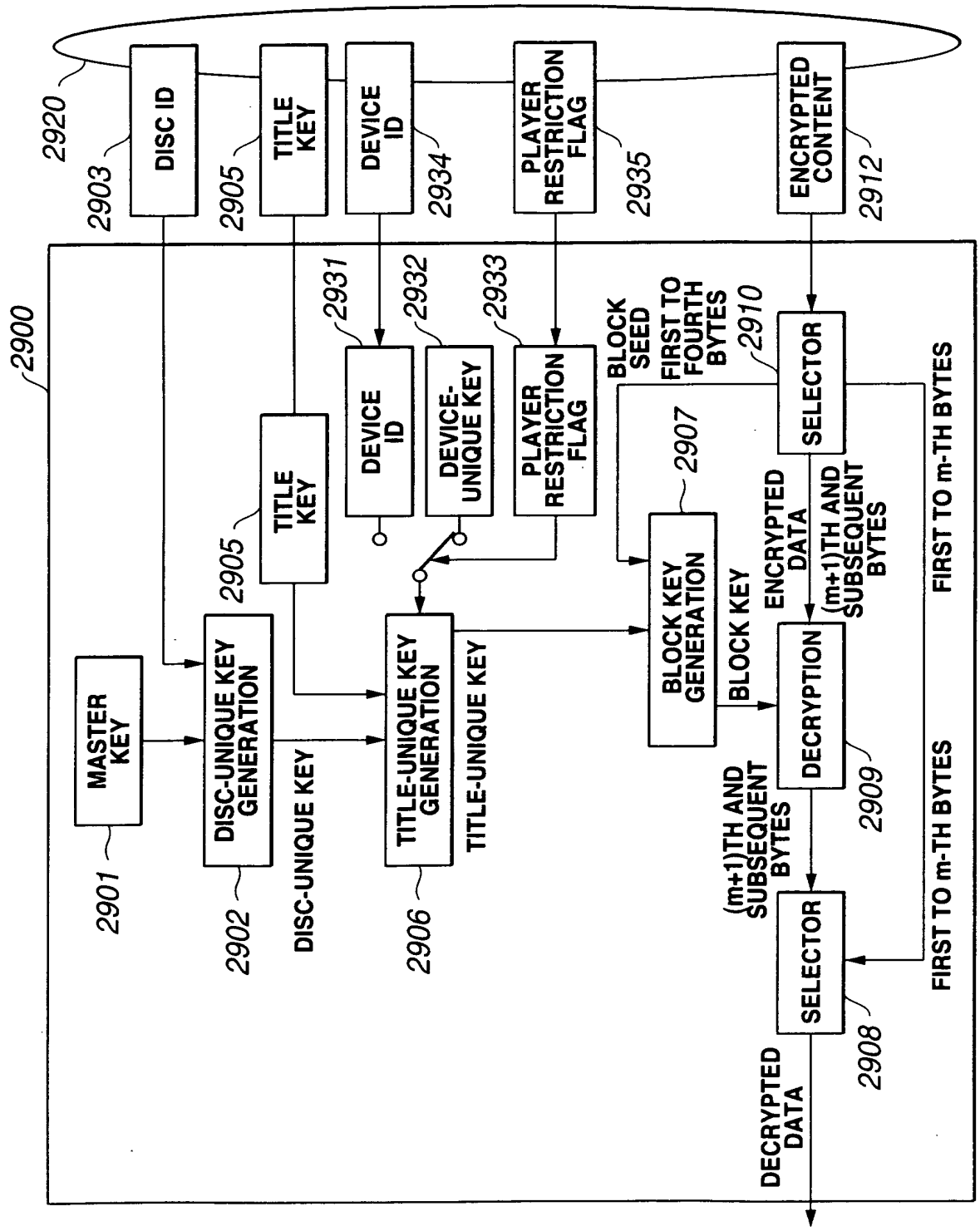

2920
2903
DISC ID
2905
TITLE KEY
2934
DEVICE ID
2935
PLAYER RESTRICTION FLAG
2912
ENCRYPTED CONTENT
2900
2931
2932
2933
BLOCK SEED
FIRST TO FOURTH BYTES
2910
SELECTOR
DEVICE ID
DEVICE-UNIQUE KEY
PLAYER RESTRICTION FLAG
2907
TITLE KEY
2905
BLOCK KEY GENERATION
BLOCK KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
MASTER KEY
DISC-UNIQUE KEY GENERATION
TITLE-UNIQUE KEY GENERATION
TITLE-UNIQUE KEY
DECRYPTION
2909
2901
2902
DISC-UNIQUE KEY
2906
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
SELECTOR
2908
DECRYPTED DATA

FIG.29

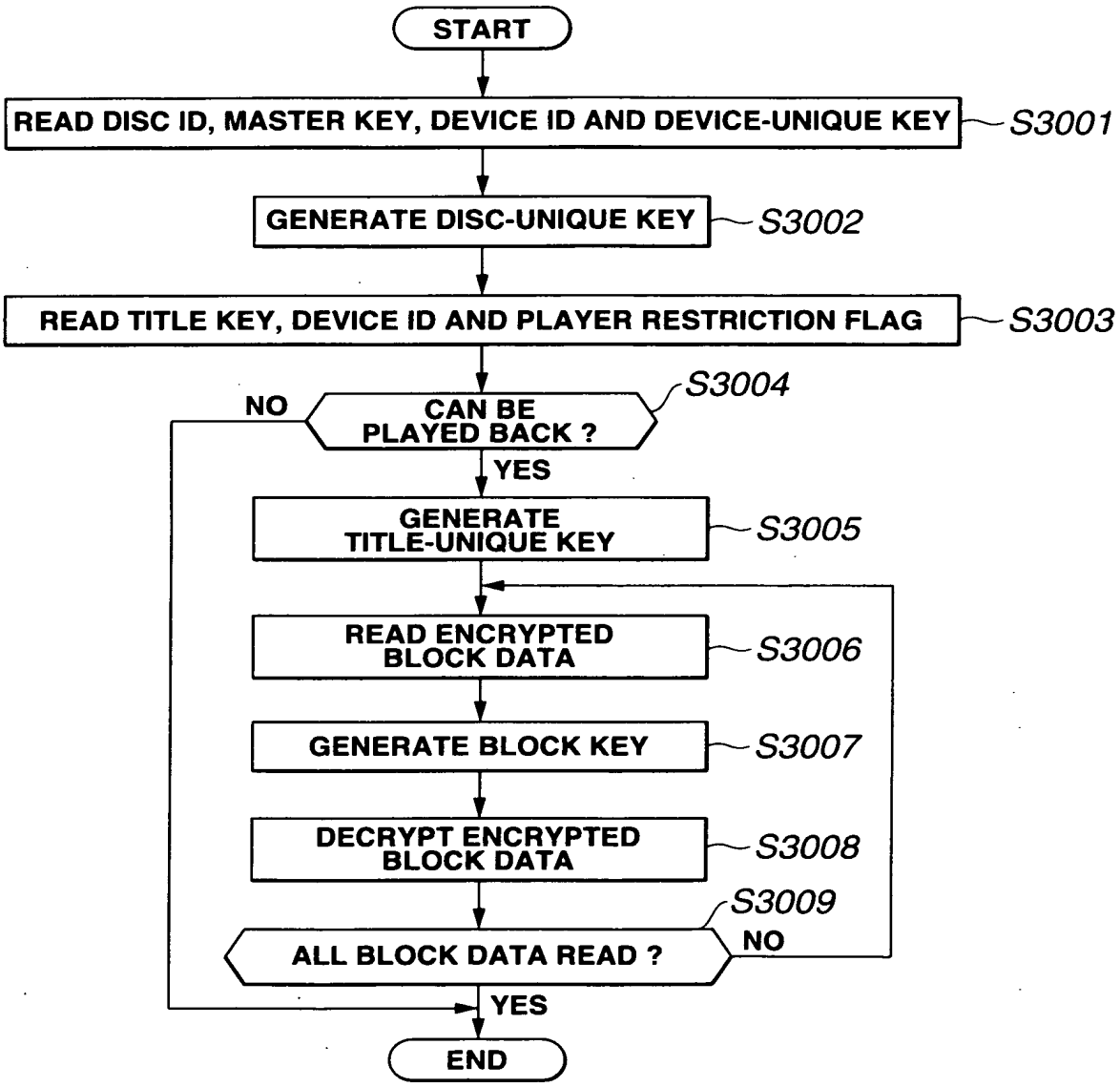

START
READ DISC ID, MASTER KEY, DEVICE ID AND DEVICE-UNIQUE KEY
S3001
GENERATE DISC-UNIQUE KEY
S3002
READ TITLE KEY, DEVICE ID AND PLAYER RESTRICTION FLAG
S3003
CAN BE PLAYED BACK ?
S3004
NO
YES
GENERATE TITLE-UNIQUE KEY
S3005
READ ENCRYPTED BLOCK DATA
S3006
GENERATE BLOCK KEY
S3007
DECRYPT ENCRYPTED BLOCK DATA
S3008
S3009
ALL BLOCK DATA READ ?
NO
YES
END

FIG.30

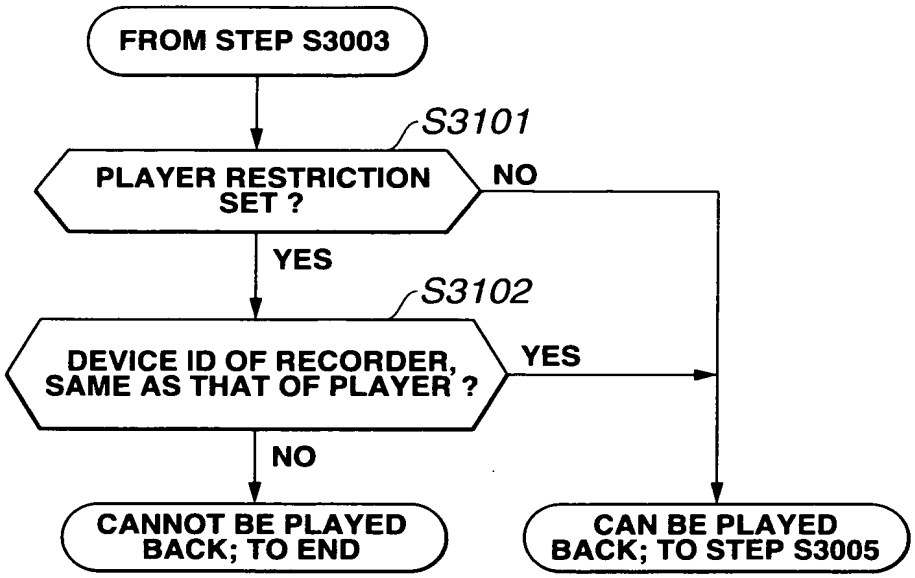

FROM STEP S3003
S3101
PLAYER RESTRICTION SET ?
NO
YES
S3102
DEVICE ID OF RECORDER, SAME AS THAT OF PLAYER ?
YES
NO
CANNOT BE PLAYED BACK; TO END
CAN BE PLAYED BACK; TO STEP S3005

FIG.31

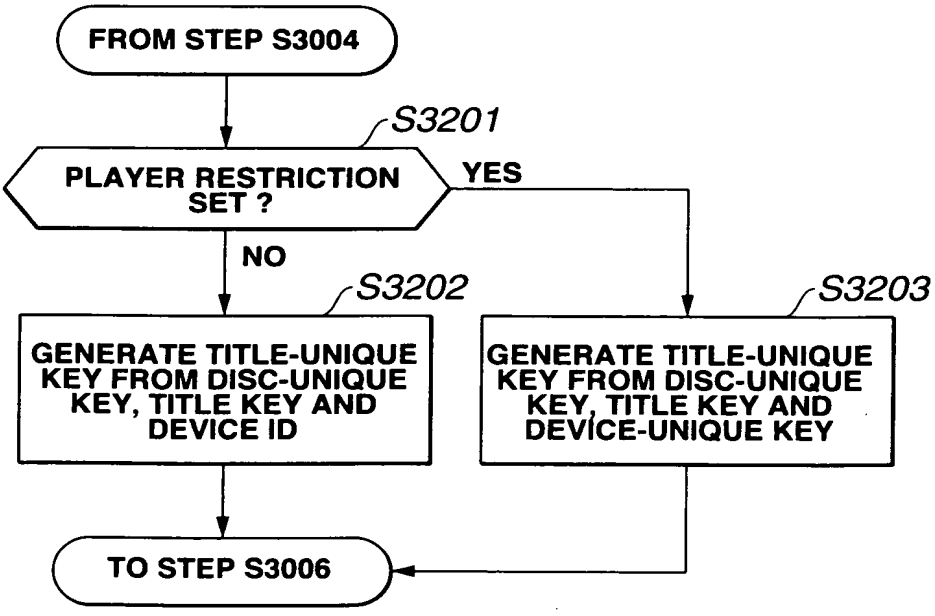

FROM STEP S3004
S3201
PLAYER RESTRICTION SET ?
YES
NO
S3202
S3203
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE ID
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE-UNIQUE KEY
TO STEP S3006

FIG.32

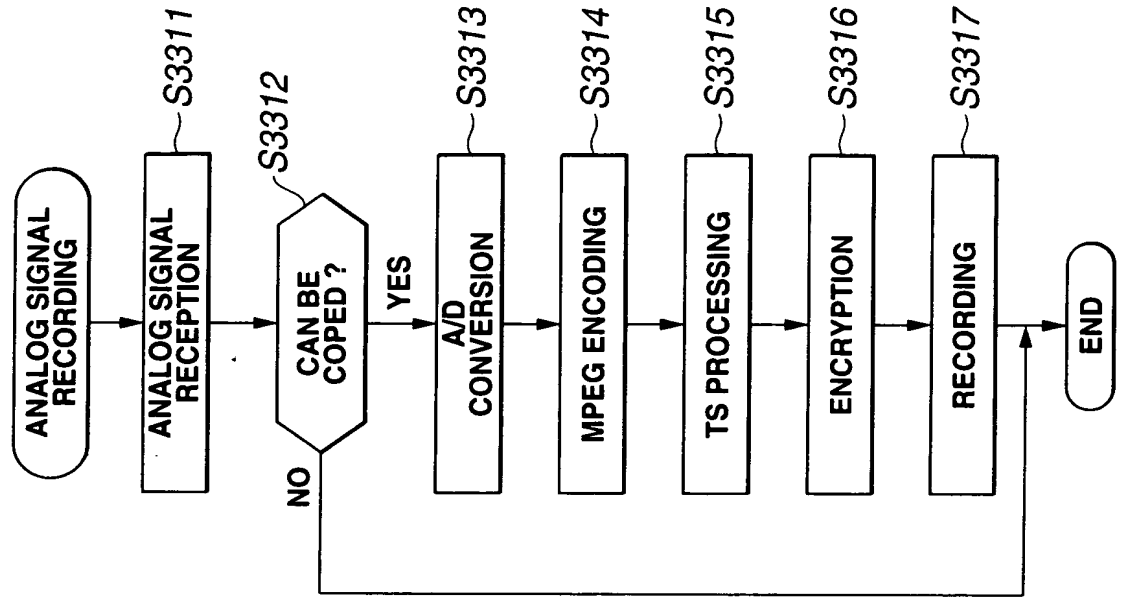


FIG.33B

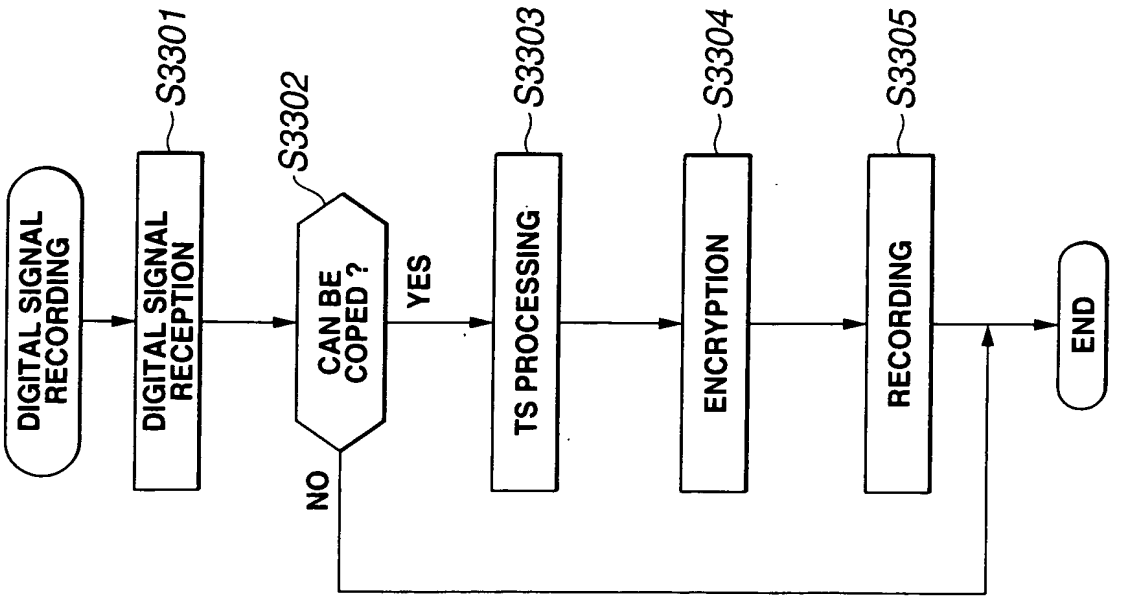


FIG.33A

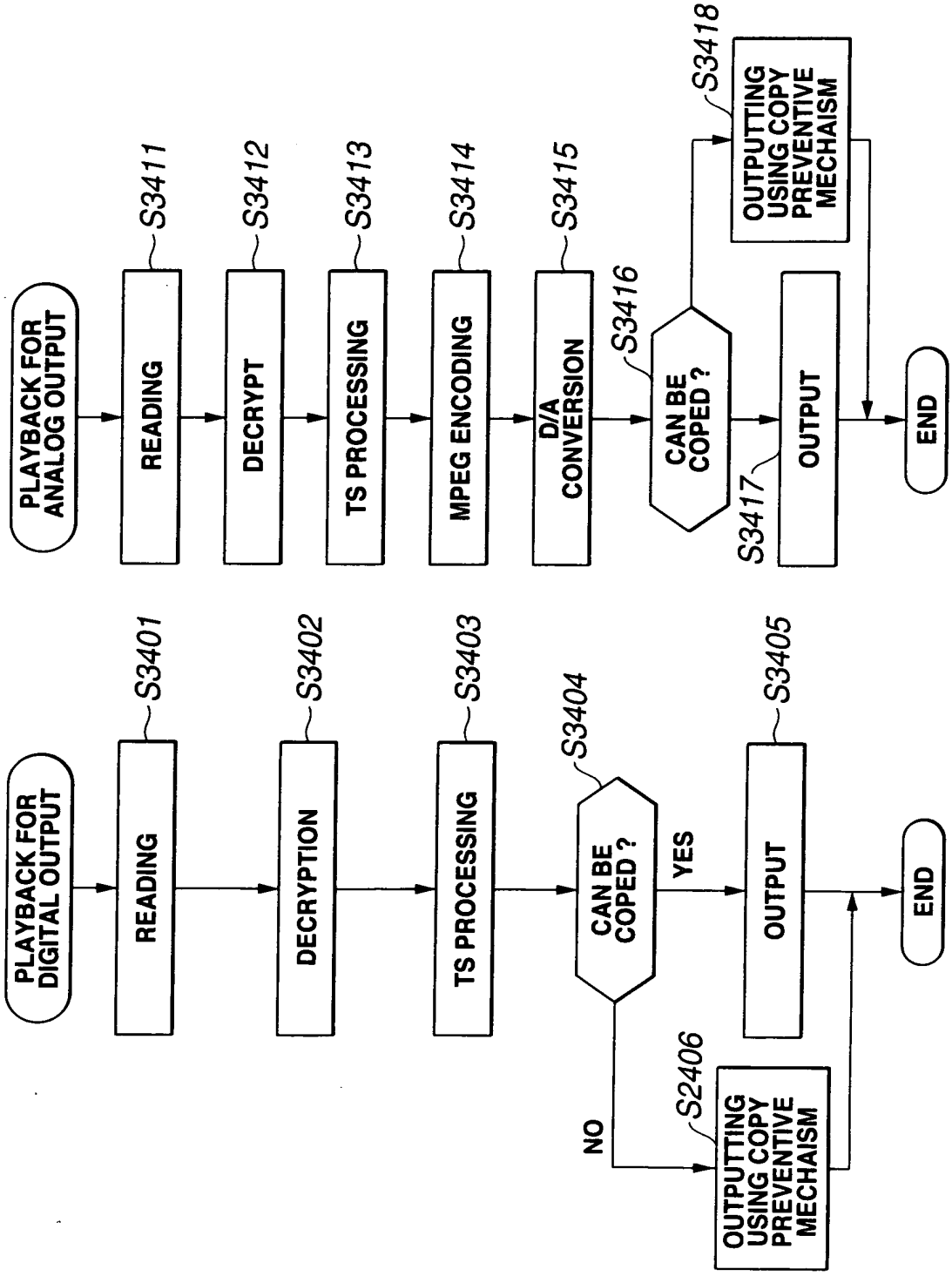


FIG.34A

FIG.34B

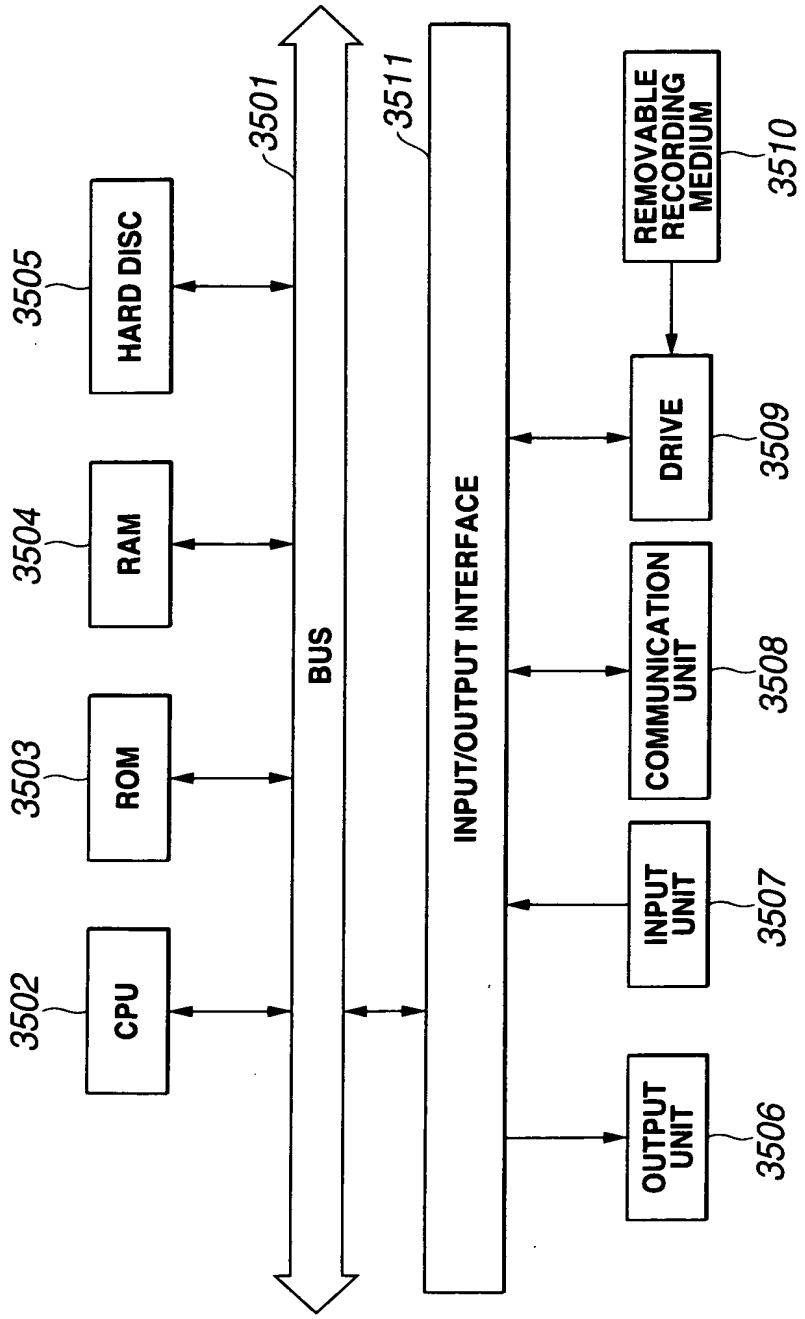

3501
3511
BUS
INPUT/OUTPUT INTERFACE
3505
HARD DISC
3504
RAM
3503
ROM
3502
CPU
REMOVABLE RECORDING MEDIUM
3510
DRIVE
3509
COMMUNICATION UNIT
3508
INPUT UNIT
3507
OUTPUT UNIT
3506

FIG.35